الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1643

(2022/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن الحوسبة السحابية – أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية

المتطلبات والمبادئ التوجيهية بشأن أمن الحاويات في بيئات الحوسبة السحابية

التوصية ITU-T X.1643

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.199–X.1
التوصيل البيني للأنظمة المفتوحة	X.299–X.200
التشغيل البيني للشبكات	X.399–X.300
أنظمة معالجة الرسائل	X.499–X.400
الدليل	X.599–X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699–X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799–X.700
الأمن	X.849–X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899–X.850
المعالجة الموزعة المفتوحة	X.999–X.900
آمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029–X.1000
أمن الشبكة	X.1049–X.1030
إدارة الأمن	X.1069–X.1050
الخصائص البيومترية	X.1099–X.1080
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1109–X.1100
أمن الشبكة المحلية	X.1119–X.1110
أمن الخدمات المتنقلة	X.1139–X.1120
أمن الويب (1)	X.1149–X.1140
أمن التطبيق (1)	X.1159–X.1150
الأمن بين جهتين نظيرتين	X.1169–X.1160
أمن معرفات الهوية عبر الشبكات	X.1179–X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1199–X.1180
آمن الفضاء السيبراني	
الأمن السيبراني	X.1229–X.1200
مكافحة الرسائل الاقتحامية	X.1249–X.1230
إدارة الهوية	X.1279–X.1250
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1309–X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1319–X.1310
أمن شبكة الكهرباء الذكية	X.1339–X.1330
البريد المعتمد	X.1349–X.1340
أمن إنترنت الأشياء (IoT)	X.1369–X.1350
أمن أنظمة النقل الذكية (ITS)	X.1399–X.1370
أمن سجل الحسابات الموزع (DLT)	X.1429–X.1400
أمن التطبيق (2)	X.1459–X.1450
أمن الويب (2)	X.1489–X.1470
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1519–X.1500
تبادل مواطن الضعف/الحالة	X.1539–X.1520
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1549–X.1540
تبادل السياسات	X.1559–X.1550
طلب المعلومات الحدسية والمعلومات الأخرى	X.1569–X.1560
تعرف الهوية والاكتشاف	X.1579–X.1570
التبادل المضمون	X.1589–X.1580
الدفاع السيبراني	X.1599–X.1590
آمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1601–X.1600
تصميم أمن الحوسبة السحابية	X.1639–X.1602
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	**X.1659–X.1640**
تنفيذ أمن الحوسبة السحابية	X.1679–X.1660
أمن أشكال أخرى للحوسبة السحابية	X.1699–X.1680
الاتصالات الكمومية	
المصطلحات	X.1701–X.1700
مولّد الأعداد العشوائية الكمومية	X.1709–X.1702
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1711–X.1710
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1719–X.1712
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1729–X.1720
آمن البيانات	
أمن البيانات الضخمة	X.1759–X.1750
حماية البيانات	X.1789-X.1770
آمن شبكات الاتصالات المتنقلة الدولية–2020	X.1819–X.1800

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1643

المتطلبات والمبادئ التوجيهية بشأن أمن الحاويات في بيئات الحوسبة السحابية

ملخص

تحلل التوصية ITU-T X.1643 التهديدات والتحديات الأمنية أمام الحاويات الافتراضية في بيئة الحوسبة السحابية وتوصف إطاراً مرجعياً مع مبادئ توجيهية أمنية بشأن الحاويات الافتراضية في الحوسبة السحابية.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1643	2022-01-07	17	11.1002/1000/14804

مصطلحات أساسية

حوسبة سحابية، مبادئ توجيهية أمنية، حاويات افتراضية.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

التوصية ITU-T X.1643

المتطلبات والمبادئ التوجيهية بشأن أمن الحاويات في بيئات الحوسبة السحابية

1 مجال التطبيق

تحلل هذه التوصية التهديدات والتحديات الأمنية أمام الحاويات الافتراضية في بيئات الحوسبة السحابية وتوصف إطاراً مرجعياً مع مبادئ توجيهية أمنية بشأن الحاويات الافتراضية في الحوسبة السحابية.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1162] التوصية ITU-T X.1162 (2008)، *معمارية الأمن في شبكان بين الأقران والتشغيلات في هذه الشبكات*.

[ITU-T X.1255] التوصية ITU-T X.1255 (2013)، *إطار لاكتشاف معلومات إدارة الهوية*.

[ITU-T X.1279] التوصية ITU-T X.1279 (2020)، *إطار للاستيقان المعزز باستخدام القياسات البيومترية عن بُعد مع آليات الكشف عن حالات الانتحال*.

[ITU-T X.1601] التوصية ITU-T X.1601 (2015)، *إطار الأمن للحوسبة السحابية*.

[ITU-T X.1605] التوصية ITU-T X.1605 (2020)، *متطلبات أمن البنية التحتية كخدمة (IaaS) عمومية في الحوسبة السحابية*.

[ITU-T X.3508] التوصية ITU-T X.3508 (2019)، الحوسبة السحابية – *نظرة عامة على الحوسبة السحابية الموزعة والمتطلبات رفيعة المستوى*.

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في مصادر أخرى:

1.1.3 التحكم في النفاذ (access control) [b-ITU-T X.800]: منع استخدام غير مرخص به لمورد ما، بما في ذلك منع استخدام مورد بطريقة غير مرخص بها.

2.1.3 صورة الخدمة السحابية (cloud service image) [ITU-T Y.3508]: شفرة قابلة للتنفيذ مع معلومات حالة الآلة (انظر الفقرة 10.1.3) أو الحاوية الافتراضية (انظر الفقرة 11.1.3).

3.1.3 بيئة التنفيذ (execution environment) [b-ITU-T Y.4500.1]: كيان منطقي يمثل بيئة قادرة على تشغيل الوحدات البرمجية.

4.1.3 البوابة (gateway) [b-ITU-T H.350.4]: جهاز يترجم من بروتوكول إلى آخر. غالباً ما تترجم البوابات بين شبكة IP والشبكة الصوتية العمومية التبديلية للسماح بدمج الاثنين.

5.1.3 التنسيق (orchestration) [b-ITU-T Y.3100]: في سياق الاتصالات المتنقلة الدولية–2020 (IMT-2020)، العمليات الهادفة إلى الترتيب التلقائي للوظائف والموارد الشبكية في البنى التحتية المادية والافتراضية، على السواء، وتنسيقها وإنشاء أمثلة لها واستخدامها تلقائياً، باستخدام معايير تحقق المستوى الأمثل من هذه العمليات.

6.1.3 الشبكة التراكبية (overlay network) [b-ITU-T X.1162]: الشبكة التراكبية هي شبكة افتراضية تعمل فوق شبكة أخرى. ومثل أي شبكة أخرى، تتكون الشبكة التراكبية من مجموعة من العقد والوصلات فيما بينها. وبما إن الوصلات منطقية، فقد تقابل العديد من الوصلات المادية للشبكة الأساسية.

7.1.3 السجل (registry) [b-ITU-T X.1255]: آلية لتسجيل البيانات الشرحية بشأن الكيانات الرقمية ومخططات حفظ البيانات الشرحية، وهي توفر القدرة على البحث في السجل عن معرفات الهوية الثابتة على أساس استخدام مخططات البيانات الشرحية.

8.1.3 الانتحال (spoofing) [b-ITU-T X.1279]: ادعاء كيان ما بأنه كيان مختلف، بتقديم صورة مسجلة أو عينة بيانات بيومترية أخرى أو خاصية بيومترية مشتقة اصطناعياً، من أجل انتحال شخصية فرد ما.

9.1.3 أمن طبقة النقل (transport layer security) [b-ITU-R BT.1699]: بروتوكول يستخدم لإرسال واستقبال البيانات المشفرة عبر الإنترنت. ويدعم هذا البروتوكول توليفة من تكنولوجيات الأمن المختلفة بما في ذلك نظام تجفير المفاتيح المشتركة والشهادات الرقمية ودوال الاختزال لمنع التنصت وتزوير الرسائل والانتحال.

10.1.3 الآلة الافتراضية (virtual machine) (VM) [b-ITU-T Q.1743]: الآلة الافتراضية برنامج حاسوبي يحاكي وحدة المعالجة المركزية في حاسوب افتراضي. والبرامج التي تنفّذها الآلة الافتراضية تُمثَّل كشفرات بايتات، وهي عمليات بدائية لهذا الحاسوب الافتراضي.

11.1.3 الحاوية الافتراضية (virtualization container) [b-ITU-T L.1362]: قسم من عقدة حاسوبية يوفر بيئة حاسوبية افتراضية معزولة.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 تعطل العقدة (node failure): خطأ يتمثل في تعذّر النفاذ إلى عقدة شبكة واحدة أو أكثر في نظام التنسيق.

2.2.3 هجمات استشفاف الرزم (packet sniffing attack): طريقة للتنصت على كل حزمة عند تدفقها عبر الشبكة بشكل غير قانوني.

3.2.3 أسلوب الشبكة الخاص بتجسير الحاوية الافتراضية (virtualization container bridge network mode): أسلوب شبكة يخصص مساحة الاسم الفردية وعنوان بروتوكول الإنترنت (IP) لكل حاوية افتراضية ويسمح للحاوية الافتراضية بالاتصال بالمضيف مباشرة.

4.2.3 هجمات الهروب من الحاوية الافتراضية (virtualization container escape attack): يحصل المهاجم بشكل غير قانوني على سلطة "التنفيذ" للحاوية الافتراضية ويستخدم هذه السلطة للحصول على السلطة الأعلى للآلة الافتراضية المضيفة (VM) أو المخدم المضيف المادي للحاوية الافتراضية.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية الاختصارات والأسماء المختصرة التالية:

ACL قائمة التحكم في النفاذ *(Access Control List)*

API السطح البيني لبرمجة التطبيقات *(Application Programming Interface)*

CPU وحدة المعالجة المركزية *(Central Processing Unit)*

DDOS رفض الخدمة الموزع *(Distributed Denial of Service)*

DOS رفض الخدمة *(Denial of Service)*

DTLS أمن طبقة نقل وحدات البيانات *(Datagram Transport Layer Security)*

IaaS البنية التحتية كخدمة *(Infrastructure as a Service)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPsec بروتوكول أمن بروتوكول الإنترنت *(IP Security protocol)*

MITM هجوم الاعتراض الوسيط *(Man-in-the-Middle)*

OS نظام التشغيل *(Operating System)*

TLS أمن طبقة النقل *(Transport Layer Security)*

VM الآلة الافتراضية *(Virtual Machine)*

VXLAN شبكة محلية افتراضية قابلة للتوسعة *(Virtual eXtensible Local Area Network)*

5 الاصطلاحات

يتعين فهم المصطلحات الأساسية التالية في هذه التوصية على النحو التالي:

وكلمة "**يجوز**" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به.

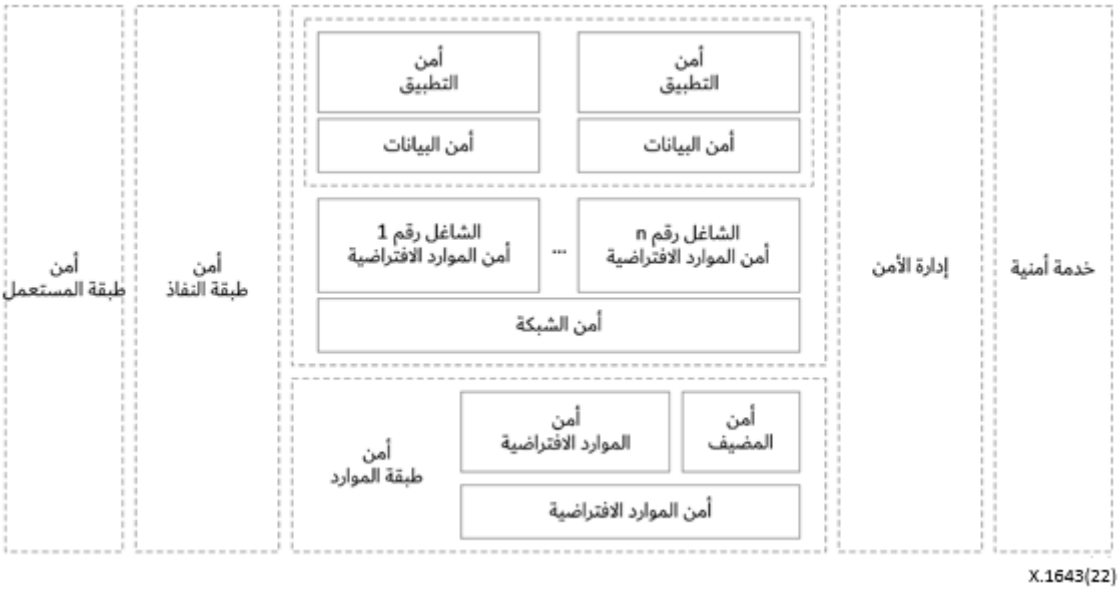
"**يجب**" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

"**ينبغي**" كلمة تدل على متطلب يوصى به لكنه غير إلزامي في المطلق. وبالتالي لا يتعين تقدم هذا المتطلب لزعم الامتثال.

"**يحظر**" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

6 نظرة عامة

توصف هذه الإطار الأمني للحاوية الافتراضية الموضح بالشكل 6-1 والذي يتضمن أمن طبقة المستعمل وأمن طبقة النفاذ وأمن طبقة الموارد وأمن طبقة الخدمة وإدارة الأمن والخدمات الأمنية.



الشكل 6-1 – الإطار الأمني للحاوية الافتراضية

ويتمثل الغرض من استخدام هذا الإطار فيما يلي:

- ضمان اعتمادية واستقرار الحاوية الافتراضية في بيئة الحوسبة السحابية،
- حماية أمن الحاوية الافتراضية من خلال حماية أمن جميع عناصر المكونات، مثل طبقة المستعمل، وطبقة النفاذ، وطبقة الموارد، وما إلى ذلك،
- توفير خدمات إدارة الأمن والأمن لعملاء خدمة الحاوية الافتراضية.

بالإشارة إلى الشكل 6-1:

أ) يدير **أمن طبقة المستعمل** أدوار المستعملين ومعلومات تعرف الهوية والعمليات من أجل ضمان التحكم في نفاذ المستعمل عبر الحاويات الافتراضية، واستيقان المستعملين وتدقيق عملياتهم.

ب) يشمل **أمن طبقة النفاذ** آليات التحكم في النفاذ، مثل النفاذ إلى الويب والنفاذ إلى السطح البيني لبرمجة التطبيقات (API).

ج) **أمن طبقة الموارد**: ينقسم أمن طبقة الموارد إلى أمن الموارد المادية وأمن المضيف وأمن الموارد الافتراضية.

'1' يشير أمن الموارد المادية إلى أمن موارد العتاد الخاص بالحاوية الافتراضية، مثل أمن الموارد الحاسوبية (وحدة المعالجة المركزية (CPU)، والذاكرة)، وموارد الشبكة (المسير، البدالة)، وموارد التخزين، وما إلى ذلك.

'2' يشير أمن المضيف إلى مخدم المضيف الذي تُطبق عليه الحاوية الافتراضية، مثل أمن نظام تشغيل (OS) المضيف، والآلة الافتراضية، إلخ.

'3' يشير أمن الموارد الافتراضية إلى أمن المكونات الافتراضية القائمة بالتمثيل الافتراضي، مثل الحوسبة الافتراضية، والشبكة الافتراضية، والتخزين الافتراضي، وما إلى ذلك.

د) تشير **إدارة الأمن** إلى وظائف إدارة الأمن للحاوية الافتراضية في بيئة الحوسبة السحابية، بما في ذلك إدارة الهوية، وإدارة الاستيقان، وإدارة السياسات الأمنية، وإدارة العمليات الأمنية، وإدارة الصيانة، وما إلى ذلك.

هـ) **خدمات الأمن**: توفير إمكانيات أمن الحاوية الافتراضية للمستعملين في شكل خدمات.

7 التحديات والتهديدات الأمنية للحاوية الافتراضية في الحوسبة السحابية

1.7 التحديات والتهديدات الأمنية الخاصة ببيئة تنفيذ الحاوية الافتراضية

بيئة تنفيذ الحاوية الافتراضية هي أول منطقة تحتاج إلى الحماية لأنها عادةً ما تكون أقل الأماكن أمناً وأسهلها لدس الشفرات الضارة. إلى جانب ذلك، يمكن أن تبرز تحديات أكثر في هذه المنطقة، على سبيل المثال، تغييرات خبيثة أو مغلوطة في الشفرات، والتعديلات الخبيثة أو الخاطئة لوحدات التحكم المدمجة المؤتمتة، أو نصوص التشكيلات المحملة بالأخطاء، أو إضافة مكتبات غير آمنة أو إصدارات غير آمنة من الشفرات الحالية.

2.7 التحديات والتهديدات الأمنية للحاوية الافتراضية أثناء أوقات التشغيل

1.2.7 التحديات والتهديدات الأمنية المتعلقة بمراقبة الحاوية الافتراضية أثناء أوقات التشغيل

حاويات المحاكاة الافتراضية سريعة الزوال. لكن هذه القيمة الأساسية تجعل مراقبتها صعبة. بالإضافة إلى ذلك، أدوات المراقبة ليس لها رؤية أو إدراك داخل الحاوية الافتراضية على مستوى السطح البيني لبرمجة التطبيقات، مما يزيد من صعوبة مراقبة سلوكيات الحاوية الافتراضية أثناء أوقات تشغيلها.

2.2.7 التحديات والتهديدات الأمنية المتعلقة بعزل الحاوية الافتراضية أثناء أوقات التشغيل

يعد العزل من الآليات الأمنية الأساسية للحاويات الافتراضية. وبالرجوع إلى التوصية [ITU-T X.1605]، الهروب من الآلة الافتراضية (VM)، والذي يعني أن مواطن الضعف في السطوح البينية بين الآلات الافتراضية التي يمكن للمهاجمين استغلالها للتحكم

في الآلة الافتراضية أو مضيف الآلة الافتراضية، كان أحد التحديات الأمنية الرئيسية للبنية التحتية كخدمة (IaaS) في الحوسبة السحابية. وبالمثل، مع العزل غير الآمن، يمكن أن يعاني محرك الحاوية الافتراضية من هجمات الهروب من الآلة الافتراضية، أي يمكن للمهاجمين استغلال حاوية افتراضية مخترقة لمهاجمة حاويات افتراضية أخرى تشترك في نفس نظام التشغيل المضيف، أو مهاجمة نظام التشغيل المضيف للشبكة التراكبية أو المضيف مباشرة.

وقد التعامل غير السليم بعد تنفيذ الحاوية الافتراضية أيضاً إلى ظهور تهديدات أمنية أخرى حرجة: 1) قد تؤدي إلى تسرب معلومات متبقية حساسة للمهاجمين؛ 2) إذا لم تتمكن من تحرير الموارد الحاسوبية أو الشبكية بشكل سليم، فقد لا تحصل الحاويات الافتراضية الأخرى على الموارد اللازمة.

3.7 التحديات والتهديدات الأمنية المتعلقة بسجل الحاوية الافتراضية

كما هو معرف في التوصية [ITU-T X.1255]، السجل هو آلية لتسجيل البيانات الشرحية بشأن الكيانات الرقمية ومخططات حفظ البيانات الشرحية، والتي توفر القدرة على البحث في السجل عن معرفات الهوية الثابتة على أساس استخدام مخططات البيانات الشرحية. وبالإضافة إلى ذلك، يحتوي سجل الحاوية الافتراضية على معلومات تعرف الهوية المهمة للتخويل. وباستخدام الضوابط الأمنية المشكلة بشكل خاطئ أو استغلال مواطن الضعف، قد يتمكن المهاجمون من النفاذ إلى سجل الحاوية الافتراضية بشكل غير قانوني وتعديل المحتوى أو حذفه بالكامل. وقد تحتوي البرمجيات المتقادمة على نقاط ضعف وقد يعاني السجل من مواطن الضعف تلك حيث يمكن للمهاجمين استغلال مواطن الضعف هذه للحصول على النفاذ عبر هجمات الباب الخلفي. بالإضافة إلى ذلك، يمكن أيضاً استغلال التشكيلات المدارة بشكل سيئ من قبل المهاجمين لاختطاف سجل الحاوية الافتراضية.

4.7 التحديات والتهديدات الأمنية لصورة الخدمة السحابية

كما هي معرفة في التوصية [ITU-T Y.3508]، صورة الخدمة السحابية هي شفرة قابلة للتنفيذ مع معلومات الحالة الخاصة بالآلة الافتراضية أو الحاوية الافتراضية، وتشمل نظام التشغيل والمكتبات وملفات البيانات والتطبيقات وما إلى ذلك وبما إن الحاويات الافتراضية يتم نشرها بناءً على صور الخدمات السحابية، فإن أمن صورة الخدمة السحابية هو الشرط المسبق لأمن الحاوية الافتراضية. وتواجه صور الخدمات السحابية التهديدات الرئيسية التالية:

أ) قد تحتوي برمجيات صور الخدمات السحابية على مواطن ضعف يمكن للمهاجمين استغلالها.

ب) مع التشكيلة غير السليمة، قد يفشل التحقق من سلامة صورة الخدمة السحابية. وبالإضافة إلى ذلك، تعتمد مسؤولية التحقق من سلامة صورة الخدمة السحابية على سيناريوهات التطبيق، حيث يتحمل موردو الخدمات السحابية المسؤولية إذا قام المستعملون بنشر الحاويات الافتراضية بناءً على صور الخدمات السحابية التي يوفرها موردو الخدمات السحابية؛ بينما يتحمل المستعملون المسؤولية إذا كانت الحاويات الافتراضية المنشورة تستند إلى صور الخدمات السحابية المتحصل عليها من مصادر أخرى، مثل التنزيل من السجل.

ج) قد يتم العبث بملفات صور الخدمات السحابية خلسة. فعلى سبيل المثال، يمكن للمهاجمين زرع باب خلفي أو برمجيات ضارة في ملفات صور الخدمات السحابية أثناء التحميل أو التنزيل.

5.7 التحديات والتهديدات الأمنية لنظام التشغيل (OS)

في بيئة الحاويات الافتراضية، "تتشارك" جميع الحاويات الافتراضية في النواة وموارد المضيف الأخرى مع النظام المضيف. لذلك، يمثل نظام التشغيل المضيف للشبكة التراكبية الهدف الأكثر أهمية للهجمات. وإذا تم اختراق نظام التشغيل، فسيتم اختراق جميع الحاويات الافتراضية أيضاً. بالإضافة إلى ذلك، يمكن تطبيق الضوابط والسياسات الأمنية المستندة إلى المضيف على كل حاوية افتراضية. وعلاوة على ذلك، فإن هجوم الهروب من الآلة الافتراضية الذي يحدث عن طريق الأخطاء في شفرة التطبيق يمكن أن يتجاوز المحرك وينفذ إلى نظام التشغيل المضيف والنواة التي تتحكم في جميع التطبيقات الأخرى.

6.7 التحديات والتهديدات الأمنية المتعلقة بنظام إدارة التنسيق في الحاوية الافتراضية

كما هو معرف في التوصية [b-ITU-T Y.3100]، فإن التنسيق هو العمليات التي تهدف إلى الترتيب والتنسيق والتشكيل والاستخدام الأوتوماتي للوظائف والموارد الشبكية لكل من البنى التحتية المادية والافتراضية من خلال معايير الاستمثال، وهو عبارة عن تكنولوجيا نمطية مستخدمة في الشبكات الافتراضية (مثل بيئات الحوسبة السحابية). وفي بيئة الحاويات الافتراضية السحابية، يتيح نظام إدارة التنسيق إدارة الحاويات الافتراضية واسعة النطاق التي يتم نشرها في السحابة، ويواجه ذلك العديد من التحديات والتهديدات الأمنية على النحو التالي:

أ) إساءة استخدام الامتيازات: إذا كانت السياسة الأمنية لنظام إدارة التنسيق لا تتبع مبدأ الامتياز الأقل، فيمكن للمستعملين الاستفادة منه وتشغيل حاويات افتراضية تتجاوز امتيازاتهم الخاصة، مما يؤدي إلى عواقب أمنية كبيرة.

ب) النفاذ غير المخول إلى سطح بيني مفتوح لبرمجة التطبيقات: تمثل السطوح البينية المفتوحة لبرمجة التطبيقات وموارد الشبكة الأخرى التي يمكن النفاذ إليها من العامة مثل منافذ الشبكة على الإنترنت أسطح هجوم جديدة. ويمكن للمهاجمين استغلال مواطن الضعف في السطوح البينية المفتوحة لبرمجة التطبيقات، مثل عدم صحة الاستيقان والتخويل، والتحقق من السلامة، وما إلى ذلك، والنفاذ إلى تنسيق الحاوية الافتراضية، وتشغيل أو تعديل الحاويات الافتراضية الخاصة بها مجدداً.

ج) إدارة تعطل العقدة: يعني تعطل العقدة أنه لا يمكن النفاذ إلى عقدة شبكة واحدة أو أكثر في نظام إدارة التنسيق. ويمكن أن يؤدي التعامل غير المناسب مع تعطل العقدة إلى التداخل مع العقد العادية الأخرى وإدارة التنسيق. ويمكن للمهاجمين الاستفادة منه بشكل ضار وتدنية أداء عمليات التنسيق.

د) إدارة التشكيلة: يقدم نظام إدارة التنسيق للحاوية الافتراضية تشكيلات مختلفة على كمية ضخمة من الأصول، وأنواع مختلفة من الخدمات، وهو ما يتطلب سياسة أمنية رفيعة المستوى لإدارة التشكيلة. وقد يؤدي الخطأ في التشكيلة إلى زيادة مساحة الأسطح الهجومية، مما يؤدي إلى مخاطر أمنية كبيرة. فعلى سبيل المثال، يمكن للمهاجمين اختراق برنامج التنسيق الداخلي من خلال تطبيقات حاوية افتراضية يمكن النفاذ إليها من قبل العامة.

7.7 التحديات والتهديدات الأمنية لشبكة الحاويات الافتراضية

يمكن تشغيل شبكة الحاويات الافتراضية في إطار أسلوبين نموذجيين للشبكة، أسلوب الشبكة الخاص بتجسير الحاوية الافتراضية وأسلوب الشبكة الخاص بتراكب الحاوية الافتراضية، للاتصال بالحاويات الافتراضية الأخرى عبر نفس المضيف، أو عبر مضيفين مختلفين، أو داخل الحاويات الافتراضية.

ويخصص أسلوب الشبكة الخاص بتجسير الحاوية الافتراضية مساحة اسم فردية وعنوان بروتوكول الإنترنت (IP) لكل حاوية افتراضية ويسمح للحاوية الافتراضية بالاتصال بالمضيف مباشرة.

وكما هي معرفة في التوصية [ITU-T X.1162]، فإن الشبكة التراكبية هي شبكة افتراضية تعمل فوق شبكة أخرى. ومثل أي شبكة أخرى، تتكون الشبكة التراكبية من مجموعة من العقد والوصلات فيما بينها. وبما إن الوصلات منطقية، فقد تقابل العديد من الوصلات المادية للشبكة الأساسية. وفي بيئة الحاوية الافتراضية السحابية، توصل الشبكة التراكبية للحاوية الافتراضية حاويات افتراضية موزعة. وهي تقوم، على وجه التحديد، ببناء شبكة تراكبية افتراضية أعلى الشبكة الأساسية لكل مضيف بواسطة تقنية الشبكة المحلية الافتراضية القابلة للتوسعة (VXLAN) لتمكين التوصيل البيني للحاويات الافتراضية والسماح للحاويات الافتراضية بالاتصال عبر المضيفين.

وتتضمن التحديات والتهديدات الأمنية الشائعة لهذين الأسلوبين الشبكيين للحاوية الافتراضية ما يلي:

- **هجمات رفض الخدمة (DoS)/رفض الخدمة الموزع (DDoS)**

تواجه شبكة الحاويات الافتراضية تهديدات هجمات رفض الخدمة (DoS)/رفض الخدمة الموزع (DDoS) من الشبكات الداخلية والخارجية:

أ) تهديدات الهجمات DoS/DDoS من الشبكات الداخلية: قد يستغل المهاجم الحاويات الافتراضية المخترقة لشن الهجمات DoS/DDoS على الحاويات الافتراضية الأخرى على نفس الشبكة، لإفساد الموارد الحاسوبية للأهداف مثل عرض النطاق ووحدات المعالجة المركزية وما إلى ذلك.

ب) تهديدات الهجمات DoS/DDoS من الشبكات الخارجية: تتشارك الحاويات الافتراضية الموجودة على نفس المضيف في نفس مكيفات الشبكة المادية. وعلاوة على ذلك، إذا أطلق المهاجم الهجمات DoS/DDoS على حاوية افتراضية مستهدفة عن طريق إرسال حجم كبير من رزم البيانات من مضيفات روبوتية، فقد لا يؤدي ذلك إلى إتلاف الحاوية الافتراضية المستهدفة فحسب، بل يؤدي أيضاً إلى إفساد عرض النطاق شبكة الآلة المضيفة، مما يؤدي إلى حدوث هجمات DDoS/DoS على المضيف وعلى الحاويات الافتراضية الأخرى أيضاً.

- **هجمات الاعتراض الوسيط**

لا توفر الحاويات الافتراضية في أساليب الشبكة المختلفة آليات تجفير في الأساس، مما يؤدي إلى تعرض الحاويات الافتراضية في الواقع لهجمات الاعتراض الوسيط (MITM). فعلى سبيل المثال، فإن الانتحال، كما هو معرف في التوصية [ITU-T X.1279]، ادعاء كيان ما بأنه كيان مختلف، بتقديم صورة مسجلة أو عينة بيانات بيومترية أخرى أو خاصية بيومترية مشتقة اصطناعياً، من أجل انتحال شخصية فرد ما، وهو من التهديدات الأمنية النمطية. فيمكن للمهاجم استغلال حاوية افتراضية مخترقة وتنفيذ هجمات انتحال على حاوية افتراضية مستهدفة على نفس الشبكة الافتراضية. وبالإضافة إلى ذلك، إذا نجح المهاجم، فيمكنه بالفعل اختطاف حركة الشبكة العادية للحاوية الافتراضية، ثم تنفيذ سلسلة من هجمات الاعتراض.

وقد تختار التطبيقات الموجودة داخل الحاويات الافتراضية القيام بالتجفير الخاص بها – باستخدام بروتوكولات مثل بروتوكول أمن طبقة النقل (TLS) أو أمن طبقة نقل وحدات البيانات (DTLS). وفي هذه الحالات، قد يختار المنفِّذ الذي يدرك أن الحركة داخل الحاوية الافتراضية – أو أن الحركة تنتقل بين حاويات افتراضية، عدم تكرار توفير التجفير. والهدف من هذا النهج هو تعظيم حماية الحركة بين الحاويات الافتراضية مع تدنية الحمل الحاسوبي المرتبط بتجفير نفس الحركة أكثر من مرة.

ويرد في الفقرتين 1.7.7 و2.7.7 وصف التهديدات الأمنية الخاصة التي يواجهها أسلوب الشبكة الخاص بتجسير الحاوية الافتراضية وأسلوب الشبكة الخاص بتراكب الحاوية الافتراضية.

1.7.7 أسلوب الشبكة الخاص بتجسير الحاوية الافتراضية

في أسلوب الشبكة الخاص بتجسير الحاوية الافتراضية، توصل الحاوية الافتراضية بشبكة افتراضية من خلال السطح البيني للشبكة الافتراضية الخاصة بها، والذي يسمح للحاوية الافتراضية بالاتصال بالمضيف مباشرة والعمل كبوابة أولية. وتُرسل حزم الشبكة الخاصة بالحاوية الافتراضية أولاً إلى البوابة الأولية ثم يتم تسييرها إلى الحاويات الافتراضية الأخرى. والحاويات الافتراضية تحت نفس الشبكة الافتراضية تُوصل بينياً.

وبدون سياسة أمنية للشبكة في أسلوب الشبكة الخاص بتجسير الحاوية الافتراضية، لا يوجد تحكم في النفاذ إلى الشبكة بين الحاويات الافتراضية. وإذا لم يكن هناك جدار حماية وآليات دفاعية أخرى للشبكة، يقيم للمهاجم في حاوية افتراضية واحدة ويمكنه شن هجمات مختلفة بسهولة على حاويات افتراضية أخرى، وذلك من خلال مثلاً الانتحال، وهجمات استشفاف الحزم، وما إلى ذلك، وهذا يؤدي إلى عواقب وخيمة، مثل تسرب المعلومات الحساسة إلخ.

لذلك، هناك مخاطر أمنية للشبكة في ظل أسلوب الشبكة الخاص بتجسير الحاوية الافتراضية في حالة عدم وجود سياسة فعالة للتحكم في الوصول إلى الشبكة بين الحاويات الافتراضية على نفس المضيف.

2.7.7 أسلوب الشبكة الخاص بتراكب الحاوية الافتراضية

ليس لأسلوب الشبكة الخاص بتراكب الحاوية الافتراضية سياسة تحكم أولية في النفاذ إلى الشبكة بالنسبة للحاويات الافتراضية. ونظراً لأن حركة الشبكة VXLAN غير مجفرة بالتغيب، فإنها تحتاج إلى استخدام بروتوكولات التسيير الأخرى، مثل بروتوكول أمن بروتوكول الإنترنت (IPsec) وما إلى ذلك، لتجفير حركة الشبكة VXLAN وضمان أمن نقل البيانات.

8 المتطلبات والمبادئ التوجيهية الأمنية للحاويات الافتراضية في بيئات الحوسبة السحابية

يوفر هذا القسم مبادئ توجيهية أمنية وفقاً للتحديات والتهديدات الأمنية للحاوية الافتراضية الموضحة في القسم 7.

1.8 المتطلبات والمبادئ التوجيهية الأمنية للحاويات الافتراضية أثناء أوقات التشغيل

أ) عند إجراء تحديث للتطبيقات أو الخدمات، يجب إيقاف الحاويات الافتراضية العاملة واستبدالها بحاويات افتراضية جديدة.

ب) ينبغي استخدام أدوات للبحث عن مواطن الضعف الشائعة في أوقات التشغيل المحددة. ويجب ترقية أي حالات معرضة للخطر.

ج) لا يجوز لأي مستعمل غير مخول النفاذ إلى البرنامج الخفي للحاوية الافتراضية.

2.8 المتطلبات والمبادئ التوجيهية الأمنية لسجل الحاويات الافتراضية

أ) ينبغي تأمين المخدم الذي يستضيف السجل لتقليل مخاطر الهجمات عليه.

ب) ينبغي تشكيل أدوات التطوير ونظام إدارة التنسيق والحاويات الافتراضية بحيث لا تُوصل بالسجلات إلا عبر القنوات المجفرة.

ج) ينبغي أن تكون السجلات مجردة من صور الخدمات السحابية غير الآمنة والضعيفة والتي يجب عدم استخدامها مجدداً.

د) ينبغي فرض الاستيقان في جميع حالات النفاذ إلى السجل للتأكد من أنه لن يتسنى إضافة صور الخدمات السحابية إلا من الكيانات الموثوقة.

3.8 المتطلبات والمبادئ التوجيهية الأمنية لصور الخدمات السحابية للحاويات الافتراضية

أ) الغرض من صور الخدمات السحابية هو إنشاء حاوية افتراضية لتطبيق أو خدمة. ولا يجوز استخدام صور الخدمات السحابية لمهام الأخرى.

ب) ينبغي التحقق من صحة توقيعات صور الخدمات السحابية قبل تنفيذ صور الخدمات السحابية للتأكد من أن صور الخدمات السحابية تأتي من مصادر موثوقة ولم يتم التلاعب بها.

ج) ينبغي تنفيذ عمليات المراقبة والصيانة المستمرة للسجلات لضمان الحفاظ على صور الخدمات السحابية داخلها وتحديثها مع تغير مواطن الضعف ومتطلبات التشكيلات.

د) ينبغي أن يستخدم النفاذ إلى صور الخدمات السحابية أسماء غير قابلة للتغيير تحدد إصدارات دقيقة من صور الخدمات السحابية.

4.8 المتطلبات والمبادئ التوجيهية الأمنية لنظام التشغيل المضيف للحاويات الافتراضية

أ) ينبغي تدنية نواقل الهجمات من خلال القضاء عليها جمعاء باستثناء الأساسي منها من البيئة المضيفة.

ب) لا يجوز الخلط بين أعباء العمل الخاصة بالحاويات الافتراضية وغير الافتراضية في نفس مثيل المضيف.

ج) ينبغي التحقق من إصدار نظام التشغيل المضيف من خلال تنفيذ ممارسات وأدوات الإدارة.

د) ينبغي تدقيق كل استيقان لنظام التشغيل.

هـ) ينبغي تشغيل الحاويات الافتراضية مع الحد الأدنى من مجموعة أذونات نظام الملفات المطلوبة. وينبغي عدم إجراء أي تغييرات على الملفات في نظام التشغيل المضيف للحاوية الافتراضية إلا بسياسات التخويل.

5.8 المتطلبات والمبادئ التوجيهية الأمنية لنظام إدارة التنسيق للحاويات الافتراضية

أ) ينبغي تركيب نظام إدارة التنسيق من مصدر رسمي وموثوق ومحدث.

ب) ينبغي تشكيل نظام إدارة التنسيق لتوفير تيسر كبير وتجاوز أوتوماتي للأعطال إلى أقصى حد ممكن.

ج) ينبغي أن يستخدم نظام إدارة التنسيق نموذج نفاذ الامتيازات الأقل حيث لا يُمنح المستعمل إلا القدرة على تنفيذ إجراءات محددة على المضيف المحدد والحاوية الافتراضية المحددة وصورة الخدمة السحابية المحددة.

د) ينبغي استخدام أساليب الاستيقان القوية، مثل فرض الاستيقان متعدد العوامل بدلاً من مجرد كلمة مرور، للحسابات الإدارية لنظام إدارة التنسيق،

هـ) ينبغي تشكيل نظام إدارة التنسيق لفصل حركة الشبكة إلى شبكات افتراضية منفصلة حسب مستوى الحساسية.

و) ينبغي تشكيل نظام إدارة التنسيق لعزل عمليات النشر لمجموعات معينة من المضيفين حسب مستويات الحساسية.

6.8 المتطلبات والمبادئ التوجيهية الأمنية للحاويات الافتراضية في أساليب الشبكة المختلفة

1.6.8 قيود الحركة بين الحاويات الافتراضية في أسلوب الشبكة الخاص بتجسير الحاوية الافتراضية

في أسلوب الشبكة الخاص بالتجسير، لا تتحكم التشكيلة الأمنية الأولية المفترضة للحاوية الافتراضية في النفاذ إلى الشبكة وتقيده. ولمنع تهديدات الهجمات DoS/DDoS المحتملة، ينبغي أن تكون هناك سياسات للتحكم في النفاذ إلى الشبكة وفقاً للمتطلبات الفعلية، بما في ذلك:

أ) ينبغي حظر الاتصالات بين الحاويات الافتراضية تماماً إن أمكن. وفي سيناريوهات تطبيقات معينة، إذا كانت جميع الحاويات الافتراضية على المضيف لا تحتاج إلى اتصالات شبكية مع بعضها البعض، فقد يتم حظر الاتصالات بين حاوية افتراضية وحاوية افتراضية عن طريق تغيير التشكيلة الأمنية المفترضة.

ب) ينبغي تنفيذ سياسات التحكم في النفاذ بين الحاويات الافتراضية: ففي بيئة الحوسبة السحابية للحاوية الافتراضية حيث يوجد شاغلون متعددون، قد يكون هناك وضع تشغل فيه حاوية افتراضية واحدة العديد من المضيفين لتطغى على عرض نطاق الحاويات الافتراضية الأخرى. ومن أجل ضمان الاتصالات المنتظمة بين الحاويات الافتراضية وتجنب الحركة غير الطبيعية التي تسببها هجمات DoS/DDoS، ينبغي تطبيق آليات تقييدية على حركة الاتصالات بين الحاويات الافتراضية.

ج) ينبغي تنفيذ آليات وسياسات للتجفير، على سبيل المثال، استخدام بروتوكول IPsec لتجفير الحركة وضمان سرية الاتصالات بين الحاويات الافتراضية، وبالتالي منع هجمات التجسس على الشبكة أو هجمات الاعتراض الوسيط.

2.6.8 التحكم في النفاذ بين الحاويات الافتراضية

أ) التحكم في النفاذ في أسلوب الشبكة الخاص بتجسير الحاوية الافتراضية

في أسلوب الشبكة الخاص بالتجسير، تسمح التشكيلة الأمنية الأولية المفترضة للحاوية الافتراضية للحاويات الافتراضية بالتوصيل بنفس الشبكة الافتراضية والاتصال ببعضها البعض مباشرة. ومن ثم، فإنه لمنع حالات النفاذ غير الاعتيادية، ينبغي تشكيل آليات وسياسات للتحكم في النفاذ حسب الطلب. بما في ذلك:

1) ينبغي تشكيل شبكات افتراضية مختلفة للحاويات الافتراضية لتحقيق العزل الشبكي بين الحاويات الافتراضية المختلفة. وسيؤدي ذلك إلى حظر حركة الاتصالات مع الشبكات الأخرى وتحقيق غرض العزل بين شبكات الحاويات الافتراضية.

2) ينبغي تنفيذ التحكم في النفاذ استناداً إلى سياسة القائمة البيضاء لضمان أمن الشبكة بين الحاويات الافتراضية، ويجب حظر الاتصالات بين الحاويات الافتراضية بالتغيب، ثم تشكيل قواعد التحكم في النفاذ حسب الطلب. ويقلل التحكم في النفاذ المستند إلى سياسة القائمة البيضاء من سطح الهجوم عن طريق استراتيجية التقليل للحد الأدنى.

ب) التحكم في النفاذ بالنسبة لأسلوب الشبكة الخاص بتراكب الحاوية الافتراضية

في أسلوب الشبكة الخاص بتراكب الحاوية الافتراضية، يمكن للحاويات الافتراضية المختلفة النفاذ إلى بعضها البعض مباشرة على نفس الشبكة الفرعية والمضيف. وينبغي إضافة قواعد النفاذ إلى قائمة التحكم في النفاذ (ACL) يدوياً في سياسات التحكم في النفاذ إلى المضيف، أو ينبغي نشر جدار حماية على المضيف، للتحكم في النفاذ من المضيفين الخارجيين إلى تطبيقات الحاويات الافتراضية الداخلية.

في البيئات السحابية الكبيرة للحاويات الافتراضية، قد لا يكون من العملي تحديث قواعد جدار الحماية يدوياً بسبب التحديثات الدينامية المتكررة للخدمات الصغرية [b-ITU-T J.1301]. ويوصى باستخدام بعض الأدوات لإدارة العملية أوتوماتيكياً، مثل التجزئة الصغرية للحاوية الافتراضية، وهي تقنية جدار حماية للحاوية الافتراضية توفر آليات عزل دقيقة لتجزئة الشبكة ويمكنها إجراء عزل التجزئة لحاوية افتراضية واحدة، وحاويات افتراضية في نفس شبكة المجموعة الفرعية، أو تطبيقات حاويات افتراضية، وتنفيذ سياسات التحكم في النفاذ إلى الشبكة وفقاً لذلك.

بيبليوغرافيا

[b-ITU-T H.350.4] Recommendation ITU-T H.350.4 (2011), *Directory services architecture for SIP*.

[b-ITU-T J.1301] Recommendation ITU-T J.1301 (2021), *Specification of cloud-based converged media service to support Internet protocol and broadcast cable television – Requirements*.

[b-ITU-T L.1362] Recommendation ITU-T L.1362 (2019), *Interface for power management in network function virtualization environments – Green abstraction Layer version 2*.

[b-ITU-T Q.1743] Recommendation ITU-T Q.1743 (2016), *IMT-Advanced references to Release 11 of LTE-Advanced evolved packet core network*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.810] Recommendation ITU-T X.810 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.

[b-ITU-T X.1162] Recommendation ITU-T X.1162 (2008), *Security architecture and operations for peer-to-peer networks*.

[b-ITU-T X.1251] Recommendation ITU-T X.1251 (2019), *A framework for user control of digital identity*.

[b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

[b-ITU-T X.1279] Recommendation ITU-T X.1279 (2020), *Framework of enhanced authentication using telebiometrics with anti-spoofing detection mechanisms*.

[b-ITU-T X.1604] Recommendation ITU-T X.1604 (2020), *Security requirements of Network as a Service (NaaS) in cloud computing*.

[b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014), *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3502] Recommendation ITU-T Y.3502 (2014), *Information technology – Cloud computing – Reference architecture*.

[b-ITU-T Y.4500.1] Recommendation ITU-T Y.4500.1 (2018), *oneM2M – Functional architecture*.

[b-ITU-R BT.1699] Recommendation ITU-R BT.1699 (2013), *Harmonization of declarative application formats for interactive TV*.

[b-ISO/IEC 19944] ISO/IEC 19944:2016, *Information technology – Cloud services and devices: Data flow, data categories and data use*.

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology –Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27729] ISO/IEC 27729:2012, *Information and documentation – International standard name identifier (ISNI)*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology –Security techniques – Privacy framework*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2022