国 际 电 信 联 盟

ITU-T X.1643

(01/2022)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

云计算安全 – 云计算安全概述

云计算环境中虚拟化容器的安全要求和导则

ITU-T X.1643 建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	**X.1640–X.1659**
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1643 建议书

云计算环境中虚拟化容器的安全要求和导则

摘要

ITU-T X.1643建议书分析了云计算环境中虚拟化容器面临的安全威胁和挑战，并为云中虚拟化容器规定了一个包括安全导则的参考框架。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1643	2022-01-07	17	11.1002/1000/14804

关键词

云计算，安全导则，虚拟化容器。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过ITU-T网址查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1643 建议书

云计算环境中虚拟化容器的安全要求和导则

1 范围

本建议书分析了云计算环境中虚拟化容器面临的安全威胁和挑战，并为云中虚拟化容器规定了一个包括安全导则的参考框架。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其他参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其他参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其他参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

[ITU-T X.1162] ITU-T X.1162建议书（2008年），对等网络的安全架构和运营。

[ITU-T X.1255] ITU-T X.1255建议书（2013年），发现身份管理信息的框架。

[ITU-T X.1279] ITU-T X.1279建议书（2020年），使用具有反欺骗检测机制的远程生物特征识别的增强认证框架。

[ITU-T X.1601] ITU-T X.1601建议书（2015年），云计算安全框架。

[ITU-T X.1605] ITU-T X.1605建议书（2020年），云计算中公共基础设施即服务（IaaS）的安全要求。

[ITU-T Y.3508] ITU-T Y.3508建议书（2019年），云计算 – 分布式云概述和高级要求。

3 定义

3.1 他处定义的术语

本建议书采用下列他处定义的术语：

3.1.1 访问控制（access control）[b-ITU-T X.800]：防止未经授权地使用资源，包括防止以未经授权的方式使用资源。

3.1.2 云服务镜像（cloud service image）[ITU-T Y.3508]：带有虚拟机（见第3.1.10节）或容器（见第3.1.11节）状态信息的可执行代码。

3.1.3 执行环境（execution environment）[b-ITU-T Y.4500.1]：表示一个能运行软件模块的环境的逻辑实体。

3.1.4 网关（gateway）[b-ITU-T H.350.4]：将一个协议转换到另一个协议的设备。通常网关会在IP网络与公共交换语音网络之间进行转换，以实现二者的集成。

3.1.5 编排（orchestration）[b-ITU-T Y.3100]：在IMT-2020背景下，旨在通过优化标准，对物理和虚拟基础设施的网络功能和资源进行自动安排、协调、实例化和使用的过程。

3.1.6 覆盖网络（overlay network）[b-ITU-T X.1162]：覆盖网络是运行在另一个网络之上的虚拟网络。像任何其他网络一样，覆盖网络包括一组节点和它们之间的链路。由于链路是逻辑链路，因此它们可对应底层网络的许多物理链路。

3.1.7 注册表（registry）[b-ITU-T X.1255]：一种对有关数字实体的元数据进行注册并存储元数据模式的机制，它提供的能力有助于在所用元数据模式基础上搜索注册表，找出持久标识符。

3.1.8 欺骗（spoofing）[b-ITU-T X.1279]：展示一幅记录的镜像或其他生物特征识别数据样本或者人工衍生的生物特征识别特性，一个实体伪装为一个不同的实体，以便冒充某个个体。

3.1.9 传输层安全（transport layer security）[b-ITU-R BT.1699]：用于在互联网上发送和接收编码数据的协议。该协议支持多种安全技术的组合，包括共享密钥密码系统、数字证书、哈希函数，以防止窃听、消息伪造和欺骗。

3.1.10 虚拟机（virtual machine（VM））[b-ITU-T Q.1743]：一个软件程序，它模拟一个假设的计算机中央处理器。由一个虚拟机执行的程序表现为字节编码，它们是这个假设的计算机的原始操作。

3.1.11 虚拟化容器（virtualization container）[b-ITU-T L.1362]：指的是一个计算节点的分区，它提供一个隔离的虚拟化计算环境。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 节点故障（node failure）：指的是一种错误，在编排系统中无法访问一个或多个网络节点。

3.2.2 分组嗅探攻击（packet sniffing attack）：当每个分组流经网络时实施非法窃听的一种方法。

3.2.3 虚拟化容器桥接网络模式（virtualization container bridge network mode）：指的是一种网络模式，它为每个虚拟化容器分配单独的命名空间和网际协议（IP）地址，并允许虚拟化容器直接与主机进行通信。

3.2.4 虚拟化容器逃逸攻击（virtualization container escape attack）：攻击者非法获取虚拟化容器的“执行”权限，并利用该权限来获取虚拟化容器主机虚拟机（VM）或物理主机服务器的更高权限。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

ACL 访问控制列表

API 应用程序编程接口

CPU 中央处理器

DDOS 分布式拒绝服务

DOS 拒绝服务

DTLS 数据报传输层安全

IaaS	基础设施即服务
IP	网际协议
IPsec	IP安全协议
MITM	中间人攻击
OS	操作系统
TLS	传输层安全
VM	虚拟机
VXLAN	虚拟可扩展局域网

5 惯例

在本建议书中：

关键词“**可以**”（**may**）表示允许作为选项但并非建议遵守的要求。

关键词“**须（shall）**”表明一项必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

关键词“**应（should）**”表明一项建议的、并非需要绝对遵守的要求，因此声称遵守本建议书并不需要按照该要求行事。

关键词“**不得（shall not）**”表明一项必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

6 概述

本建议书规定了一个如图6-1所示的虚拟化容器安全框架，它包括用户层安全、接入层安全、资源层安全、服务层安全、安全管理和安全服务。

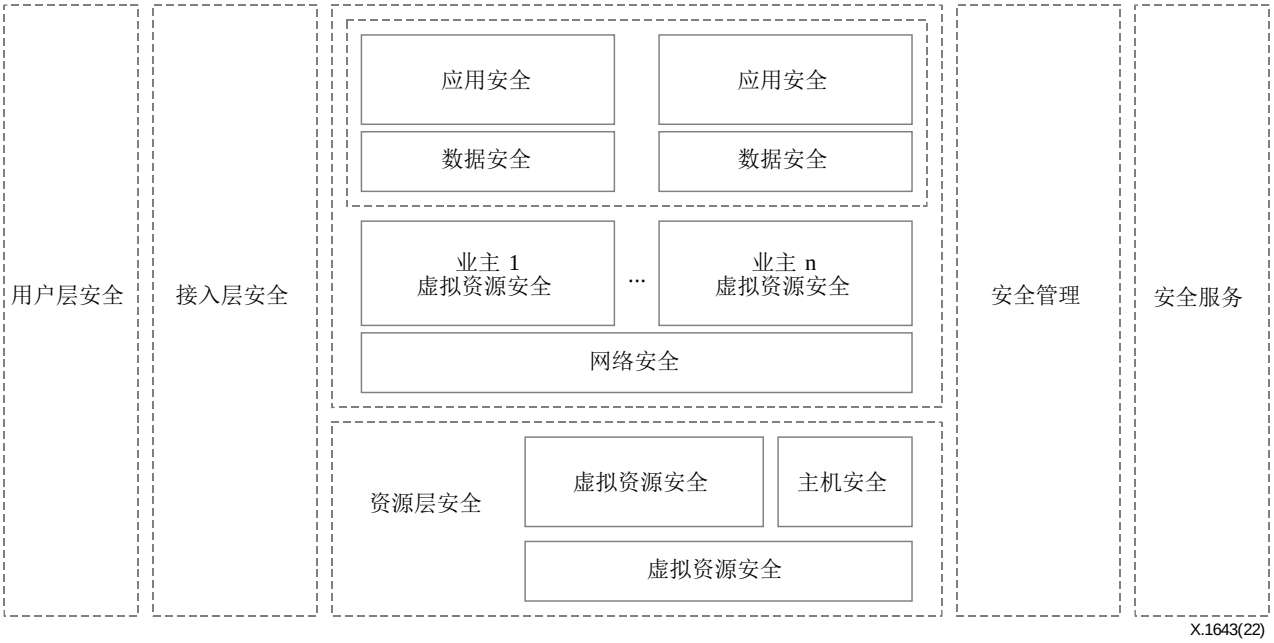

图6-1 – 虚拟化容器安全框架

使用本框架的目的是：

– 确保云计算环境中虚拟化容器的可靠性和稳定性；

– 通过保护所有组件元素（例如，用户层、接入层、资源层等）的安全，来保护虚拟化容器的安全；以及

– 为虚拟化容器服务客户端提供安全管理和安全服务。

参考图6-1：

a) **用户层安全**管理用户的角色、识别信息和操作，以确保用户对虚拟化容器的访问控制，对用户进行认证以及对用户操作进行审计。

b) **接入层安全**包括访问控制机制，例如，万维网访问、应用程序编程接口（API）访问。

c) **资源层安全**：资源层安全分为物理资源安全、主机安全和虚拟资源安全。

   i. **物理资源安全**指的是虚拟化容器硬件资源的安全，例如，计算资源（中央处理器（CPU）、内存）、网络资源（路由器、交换机）、存储资源等的安全。

   ii. **主机安全**指的是实现虚拟化容器的主机服务器，例如，主机操作系统（OS）、VM等的安全。

   iii. **虚拟资源安全**指的是虚拟化的虚拟组件的安全，例如，虚拟计算、虚拟网络、虚拟存储等。

d) **安全管理**是指云计算环境中虚拟化容器的安全管理功能，包括身份管理、认证管理、安全策略管理、安全运营管理、维护管理等。

e) **安全服务**：以服务的形式为用户提供虚拟化容器安全能力。

7 云计算中虚拟化容器面临的安全挑战和威胁

7.1 虚拟化容器执行环境面临的安全挑战和威胁

虚拟化容器执行环境是首先需要保护的区域，因为它通常是最不安全和最容易插入恶意代码的地方。此外，该处可能遭遇更多威胁，例如，恶意的或愚蠢的源代码更改、对自动构建控制器的恶意或错误更改、错误加载配置脚本，并添加不安全的库或现有代码的不安全版本。

7.2 运行时虚拟化容器面临的安全挑战和威胁

7.2.1 虚拟化容器运行时监测面临的安全挑战和威胁

虚拟化容器是短命的，但该核心价值使监测变得困难。此外，监测工具在API层面在虚拟化容器内部不可见或无感知，这使在其运行时监测虚拟化容器行为变得更加困难。

7.2.2 虚拟化容器运行时隔离面临的安全挑战和威胁

隔离是虚拟化容器的核心安全机制。参见[ITU-T X.1605]，虚拟机（VM）逃逸，这意味着攻击者可用来控制VM或VM主机的VM之间接口的漏洞是云计算中基础设施即服务（IaaS）面临的主要安全挑战之一。同样，因为不安全的隔离，虚拟化容器引擎可能会遭受虚拟化容器逃逸攻击，即攻击者可利用遭破坏的虚拟化容器来攻击共享同一主机操作系统的其他虚拟化容器，并进一步直接攻击底层主机操作系统或主机。

虚拟化容器执行后处理不当还可能引入其他严重的安全威胁：1) 可能会将敏感的残留信息泄露给攻击者；2) 如果不能正确释放计算或网络资源，那么其他虚拟化容器可能无法获得所需的资源。

7.3 虚拟化容器注册表面临的安全挑战和威胁

如[ITU-T X.1255]中所定义，注册表是一种用于注册有关数字实体的元数据和存储元数据模式的机制，它提供了基于元数据模式的使用在注册表中搜索持久标识符的能力。此外，虚拟化容器的注册表包含有关授权的重要标识信息。通过错误配置的安全控制或漏洞利用，攻击者可能会非法访问虚拟化容器的注册表并完全更改或删除内容。过时的软件可能存在漏洞，注册表可能会受到这些漏洞的影响，因为攻击者可以利用其漏洞通过后门攻击来获得访问权限。此外，管理不善的配置也可能被攻击者用来劫持虚拟化容器的注册表。

7.4 云服务镜像面临的安全挑战和威胁

如[ITU-T Y.3508]中所定义，云服务镜像指的是带有虚拟机或虚拟化容器状态信息的可执行代码，并包括操作系统、库、数据文件、应用程序等。由于虚拟化容器是基于云服务镜像部署的，因此云服务镜像安全是虚拟化容器安全的前提条件。云服务镜像面临以下主要威胁：

a) 云服务镜像的软件可能包含可被攻击者利用的漏洞。

b) 若配置不当，可能无法验证云服务镜像完整性检查结果。此外，有关验证云服务镜像完整性的问责制取决于应用场景，当中如果用户基于云服务提供商提供的云服务镜像来部署虚拟化容器，那么由云服务提供商来负责；而如果部署的虚拟化容器基于来自其他地方的云服务映像，例如，下载自注册表，那么由用户来负责。

c) 云服务镜像文件可能被偷偷地篡改。例如，攻击者可以在上载或下载过程中将后门或恶意软件植入到云服务镜像文件中。

7.5 操作系统（OS）面临的安全挑战和威胁

在虚拟化容器化环境中，所有虚拟化容器都与主机系统“共享”内核和其他主机资源。因此，底层主机操作系统是最关键的攻击目标。如果操作系统遭到破坏，那么所有虚拟化容器也会受到损害。此外，可以在每个虚拟化容器上应用基于主机的控制和安全策略。另外，通过应用程序代码中的缺陷发生的虚拟化容器逃逸攻击可以绕过引擎并访问用于控制所有其他应用程序的主机操作系统和内核。

7.6 虚拟化容器编排管理系统面临的安全挑战和威胁

如[b-ITU-T Y.3100]中所定义，编排指的是旨在通过优化标准自动安排、协调、实例化和使用物理与虚拟基础设施的网络功能和资源的过程，它是一种用在虚拟网络（例如，云计算环境）中的典型技术。在云虚拟化容器环境中，编排管理系统实现对部署在云中的大规模虚拟化容器的管理，它面临以下几个安全挑战和威胁：

a) 权限滥用：如果编排管理系统的安全策略不遵循最小权限原则，那么用户可能会利用它并超越自己的权限来操作虚拟化容器，从而导致严重的安全后果。

b) 未经授权访问开放API：开放API和其他可公开访问的网络资源（例如，互联网上的网络端口）暴露新的攻击面。攻击者可利用开放API的漏洞，例如，不正确的认证、授权、完整性检查等，访问虚拟化容器编排，并进一步操作或修改其虚拟化容器。

c) 节点故障管理：节点故障意味着在编排管理系统中无法访问一个或多个网络节点。节点故障处理不当可能会干扰其他正常节点和编排管理。攻击者可能会恶意地利用它并降低编排的性能。

d) 配置管理：虚拟化容器编排管理系统针对海量资产和各类服务引入了不同的配置，这需要高水平的配置管理安全策略。错误配置可扩大攻击面并导致重大的安全风险。例如，攻击者可通过可公开访问的虚拟化容器应用程序渗透到内部编排软件中。

7.7 虚拟化容器网络面临的安全挑战和威胁

虚拟化容器网络可以运行在两种典型的网络模式下，即虚拟化容器桥接网络模式和虚拟化容器覆盖网络模式，以与同一主机上、不同主机上或虚拟化容器内的其他虚拟化容器进行通信。

虚拟化容器桥接网络模式为每个虚拟化容器分配单独的命名空间和网际协议（IP）地址，并允许虚拟化容器直接与主机进行通信。

如[ITU-T X.1162]中所定义，覆盖网络是运行在另一个网络之上的虚拟网络。像任何其他网络一样，覆盖网络包括一组节点和它们之间的链路。由于链路是逻辑链路，因此它们可能对应底层网络的许多物理链路。在云虚拟化容器环境中，虚拟化容器覆盖网络连接分布式虚拟化容器。具体来说，它通过虚拟可扩展局域网（VXLAN）技术在每台主机的底层网络之上构建一个虚拟覆盖网络，以实现虚拟化容器的互联，并允许虚拟化容器跨主机进行通信。

虚拟化容器这两种网络模式的常见安全挑战和威胁包括：

– **拒绝服务（DoS）/分布式拒绝服务（DDoS）攻击：**

虚拟化容器网络面临来自内部和外部网络的DoS/DDoS攻击威胁：

a) 来自内部网络的DoS/DDoS威胁：攻击者可能利用受损的虚拟化容器来对同一网络上的其他虚拟化容器发起DoS/DDoS攻击，以压垮诸如带宽、CPU等目标的计算资源。

b) 来自外部网络的DoS/DDoS威胁：同一主机上的虚拟化容器共享相同的物理网络适配器。此外，如果攻击者通过僵尸网络主机发送大量数据分组，来对目标虚拟化容器发起DoS/DDoS攻击，那么不仅可能破坏目标虚拟化容器，而且可能压垮主机的网络带宽，导致DoS/DDoS攻击主机和其他虚拟化容器。

– **中间人攻击：**

各种网络模式下的虚拟化容器最初都未提供加密机制，这导致虚拟化容器实际上易受到中间人攻击（MITM）。例如，如[ITU-T X.1279]中所定义，欺骗指的是通过展示一幅记录的镜像或其他生物特征识别数据样本或者人工衍生的生物特征识别特性，一个实体伪装为一个不同的实体，以便冒充某个个体，这是一种典型的威胁。攻击者可利用组成的虚拟化容器并对同一虚拟网络上的目标虚拟化容器进行欺骗攻击。此外，如果成功，攻击者实际上可以劫持虚拟化容器的正常网络流量，然后进行一系列中间人攻击。

虚拟化容器内的应用程序可以选择自己进行加密 – 使用诸如传输层安全（TLS）或数据报传输层安全（DTLS）等协议。在这些情况下，了解虚拟化容器内流量（或者在虚拟化容器之间移动的流量）的实施者可能会选择不重复提供加密。这种方法的目标是最大限度地保护虚拟化容器间的流量，同时最大限度地减少与多次加密相同流量相关的计算开销。

虚拟化容器桥接网络模式和虚拟化容器覆盖网络模式面临的具体安全威胁在第7.7.1和7.7.2节中予以描述。

7.7.1 虚拟化容器桥接网络模式

在虚拟化容器桥接网络模式下，虚拟化容器通过其虚拟网络接口连接到虚拟网络，这使虚拟化容器可直接与主机进行通信，并充当初始网关。虚拟化容器的网络分组将首先被发送到初始网关，而后路由到其他虚拟化容器。同一虚拟网络下的虚拟化容器是相互连接的。

如果虚拟化容器桥接网络模式没有网络安全策略，那么虚拟化容器之间就没有网络访问控制。如果没有防火墙等网络防御机制，那么攻击者坐在一个虚拟化容器中，就可容易地对其他虚拟化容器发起各种攻击，例如，通过欺骗、分组嗅探攻击等，这将造成诸如敏感信息泄露等严重后果。

因此，如果在同一主机上的虚拟化容器之间没有有效的网络访问控制策略，那么在虚拟化容器桥接网络模式下就存在网络安全风险。

7.7.2 虚拟化容器覆盖网络模式

虚拟化容器覆盖网络模式没有虚拟化容器的初始网络访问控制策略。另外，由于VXLAN网络流量默认不加密，因此需要利用其他隧道协议，如IP安全协议（IPsec）等，来对VXLAN网络流量进行加密并确保数据传输的安全。

8 云计算环境中虚拟化容器的安全要求和导则

本节根据第7节中描述的虚拟化容器面临的安全挑战和威胁来提供安全要求和导则。

8.1 运行时虚拟化容器的安全要求和导则

a) 更新应用程序或服务时，须停止运行的虚拟化容器并用新的虚拟化容器进行替换。

b) 应使用工具来查找在部署的运行时中的常见漏洞。对任何有风险的实例都应予升级。

c) 未经授权的用户不得访问虚拟化容器守护进程。

8.2 虚拟化容器注册表的安全要求和导则

a) 托管注册表的服务器应被锁定，以便缓解彼处受到攻击的风险。

b) 开发工具、编排管理系统和虚拟化容器应被配置为仅经加密信道连接注册表。

c) 应删除注册表中不再使用的不安全、易受攻击的云服务镜像。

d) 对注册表的所有访问都应要求认证，以确保仅可将来自可信实体的云服务镜像添加到其中。

8.3 虚拟化容器云服务镜像的安全要求和导则

a) 云服务镜像的目的是创建应用程序或服务虚拟化容器。不得使用用于其他任务的云服务映像。

b) 在执行云服务镜像之前，应对云服务镜像签名进行验证，以确保云服务镜像来自可信来源且未被篡改。

c) 应实施对注册表的持续监测和维护，以确保其中的云服务映像在漏洞和配置要求发生变化时得到维护和更新。

d) 访问云服务镜像应使用不可变的名称，这些名称指定云服务镜像的离散版本。

8.4 虚拟化容器主机操作系统（OS）的安全要求和导则

a) 应通过消除主机环境中除基本要素以外的所有要素来最小化攻击向量。

b) 不得在同一主机实例上混合虚拟化容器化和非虚拟化容器化工作负载。

c) 应通过实施管理实践和工具对主机操作系统的版本进行验证。

d) 应对操作系统的所有认证进行审计。

e) 虚拟化容器应以所需的最少文件系统权限集进行运行。虚拟化容器主机操作系统中的任何文件更改仅能通过授权策略来进行。

8.5 虚拟化容器编排管理系统的安全要求和导则

a) 编排管理系统应从官方的、可信的、最新的来源来安装。

b) 应对编排管理系统进行配置，以尽可能高地提供可用性和自动故障切换。

c) 编排管理系统应使用最小权限访问模型，当中仅授予用户在特定主机、虚拟化容器和云服务镜像上执行特定操作的能力。

d) 对编排管理系统的管理帐户应使用强认证方法，例如，要求多因素认证而不仅仅是一个密码。

e) 编排管理系统应配置为按敏感度等级将网络流量分离到离散的虚拟网络中。

f) 编排管理系统应配置为按敏感度等级将部署隔离到特定主机集中。

8.6 不同网络模式下虚拟化容器的安全要求和导则

8.6.1 虚拟化容器桥接网络模式的虚拟化容器间的流量限制

在桥接网络模式下，虚拟化容器默认的初始安全配置不控制和限制网络访问。为了防范潜在的DoS/DDoS威胁，应根据实际要求制定网络访问控制策略，包括：

a) 如果可能，须完全禁止虚拟化容器间通信。在特定的应用场景中，如果主机上的所有虚拟化容器之间都不需要网络通信，那么可通过修改默认的安全配置来禁止虚拟化容器到虚拟化容器的通信。

b) 应实施虚拟化容器间访问控制策略：在存在多租户的虚拟化容器云环境中，可能会出现单个虚拟化容器占用多台主机以压垮其他虚拟化容器带宽的情形。为了确保虚拟化容器之间的正常通信，并避免DoS/DDoS攻击导致的流量异常，应对虚拟化容器之间的通信流量实施限制机制。

c) 应实施加密机制和策略，例如，利用IPsec协议对流量进行加密，并确保虚拟化容器间通信的机密性，从而防止受到网络嗅探或中间人攻击。

8.6.2 虚拟化容器间的访问控制

a) 虚拟化容器桥接网络模式的访问控制

在桥接网络模式下，虚拟化容器默认的初始安全配置允许虚拟化容器连接到同一虚拟网络并直接进行相互通信。因此，为了防止异常访问，应按需配置访问控制机制和策略。包括：

1) 应为虚拟化容器配置不同的虚拟网络，以实现不同虚拟化容器之间的网络隔离。它将阻断与其他网络的通信流量，并实现虚拟化容器网络之间的隔离目的。

2) 应实施基于白名单策略的访问控制，以确保虚拟化容器之间的网络安全，应默认禁止虚拟化容器之间的通信，而后按需配置访问控制规则。基于白名单策略的访问控制通过最小化策略来减少攻击面。

b) 虚拟化容器覆盖网络模式的访问控制

在虚拟化容器覆盖网络模式下，不同的虚拟化容器可以在同一子网和主机上直接相互访问。访问控制列表（ACL）访问规则应手动添加到主机访问控制策略中，或者在主机上部署防火墙，以控制从外部主机到内部虚拟化容器应用程序的访问。

在大型虚拟化容器云环境中，由于微服务动态更新频繁[ITU-T J.1301]，手动更新防火墙规则可能不切实际。建议使用一些工具来自动管理进程，例如，虚拟化容器微分段，这是一种虚拟化容器防火墙技术，提供了细粒度的网络分段隔离机制，可对单个虚拟化容器、同一子集网络中的虚拟化容器或虚拟化容器应用程序执行分段隔离，并可相应地实施网络访问控制策略。

参考书目

[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*.

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2022年，日内瓦