章节	二级目录	三级目录	知识点	页数
D1 云计算概念和体系架构	1.1 简介			
	1.2 概述	1.1.1 定义云计算	云计算是一种新的运作模式和一组用于管理计算资源共享池的技术	9
			NIST 与 ISO/IEC 定义	9
			抽象/调配	9
		1.1.2 定义模型	五个基本特征（资源池、按需自动配置、广泛的网络访问、快速弹性、提供可测量的服务）	11
			ISO/IEC 1788 六个基本特征、多租户	12
			三个服务模型（SaaS、 PaaS、 IaaS）	12
			四个部署模型（公有云、社区云、私有云、混合云）	13
		1.1.3 参考和架构模型	服务设施即服务（IaaS）	16
			平台即服务（PaaS）	18
			软件即服务（SaaS）	19

<table>
<tr><td rowspan="13">D7 基础设施安全</td><td>7.1 概述</td><td></td><td>基础设施两个层面（构建云的基础资源，云用户管理的虚拟/抽象基础设施）</td><td>80</td></tr>
<tr><td>7.2 云网络虚拟化</td><td></td><td>服务网络、存储网络、管理网络</td><td>81</td></tr>
<tr><td rowspan="6">7.3 云网络带来的安全变化</td><td>7.3.1 虚拟设备的挑战</td><td></td><td>83</td></tr>
<tr><td>7.3.2 SDN的安全优势</td><td>隔离更容易、SDN防火墙</td><td>84</td></tr>
<tr><td rowspan="2">7.3.3 微分段和软件定义的边界</td><td>只在需要时连接这些网络，降低爆炸半径</td><td>85</td></tr>
<tr><td>SDP三个组件（SDP客户机、SDP控制器、SDP网关）</td><td>85</td></tr>
<tr><td rowspan="2">7.3.4 云提供商或私有云的其他注意事项</td><td>多租户环境的分区和隔离</td><td>86</td></tr>
<tr><td>供应商还必须向云用户暴露安全控制措施，以便他们能够正确配置和管理其网络安全 性。</td><td>87</td></tr>
<tr><td>7.3.5 混合云的考虑</td><td>混合云连接架构是“堡垒”或“中转”虚拟网络</td><td>87</td></tr>
<tr><td rowspan="3">7.4 云计算与负载安全</td><td></td><td>计算抽象类型（虚拟机、容器、基于平台的负载、无服务器计算）</td><td>89</td></tr>
<tr><td>7.4.1 云对负载安全的改变</td><td></td><td></td></tr>
<tr><td>7.4.2 不可变负载增强安全性</td><td>安全性提升与需求</td><td>91</td></tr>
</table>

D8 虚拟化和容器	8.1 概述	8.1.2 网络	云提供商主要负责建立安全的网络基础设施并正确配置。	101
			云消费者主要负责合理配置虚拟网络的部署，尤其是虚拟防火墙。	101
		8.1.3 存储	在不同的地方保存了多个数据副本	102
		8.1.4 容器	容器是高度可移植代码执行环境	103
			三个组件（容器执行环境、自动协调及调度控制器、容器镜像或代码的可执行仓库）	103
			容器安全（底层物理基础设施、管理器、镜像仓库、安全性构建到容器内运行的任务/代码中）	103
			容器不一定提供完整的安全性隔离，但一定提供任务隔离。	104
	8.3 建议			104
D9 事件响应	9.0 介绍			106
	9.1 概述	9.1.1 事件响应声明周期	准备（建立事件响应能力，使组织对事件响应作好充分准备）、检测与分析、遏制，根除和恢复、总结	107
		9.1.2 云计算如何影响事件响应	准备	
			云应急工具包	109

<table>
<tr><td rowspan="3">D9 事件响应</td><td>9.1 概述</td><td rowspan="2">9.1.2 云计算如何影响事件响应</td><td>检测与分析</td><td>109</td></tr>
<tr><td></td><td>遏制、根除和恢复，始终确保云管理平面/元结构远离攻击者</td><td>111</td></tr>
<tr><td>9.2 建议</td><td></td><td></td><td>112</td></tr>
<tr><td rowspan="5">D10 应用安全</td><td rowspan="2">10.0 介绍</td><td rowspan="2">云计算主要为应用程序带来安全优势</td><td>机会（更高的安全基线、响应能力、隔离环境、独立的虚拟机、弹性、DevOps、统一接口）</td><td>113</td></tr>
<tr><td>挑战：
1. 可见性受限-收集与 安全相关的数据
2. 增加应用范围-管理平台/元结构安全性，直接影响与该云帐户相关联的任何应用程序 的安全性
3. 不断变化的威胁模型-威胁模型还需要对云提供程序或平台的技术问题进行调整
4. 降低透明度-不知道外部服务的安全控制</td><td>114</td></tr>
<tr><td rowspan="3">10.1 概述</td><td>10.1.1 安全软件开发声明周期和云计算简介</td><td>安全的设计和开发、安全部署、安全操作</td><td>115</td></tr>
<tr><td>10.1.2 安全设计与开发</td><td>五个阶段（训练、定义、设计、开发、测试）</td><td>116</td></tr>
<tr><td rowspan="2">10.1.3 安全部署</td><td>安全性测试可能会潜在的集成到开发和部署中（代码审查、单元测试，回归测试和功能测试、静态应用安全测试(SAST)、动态应用安全测试(DAST)）</td><td>117</td></tr>
<tr><td>对脆弱性评估的影响</td><td>118</td></tr>
</table>

D11 数据安全和加密	11.1 概述	11.1.2 云数据存储类型	数据分散（分为碎片）	125
		11.1.3 管理数据迁移	迁移监视云使用情况和任何数据传输（CASB、URL 过滤、DLP）	126
			保护云数据传输安全	127
		11.1.4 保护云中数据	云数据访问控制（管理平面、公共和内部共享控制、应用程序级别控制）	128
			存储(At-Rest)加密和令牌	129
			IaaS加密： 1. 卷存储加密（实例管理的加密、外部管理加密） 2. 对象和文件存储（客户端加密、服务器端加密、代理加密）	130
			PaaS 加密： 1. 应用层加密 2. 数据库加密 3. 其他	131
			SaaS 加密： 1. 提供商管理的加密 2. 代理加密	131
			密钥管理(包括客户管理的密钥)：HSM /设备、虚拟设备/软件、云提供商服务、混合	131

<table>
<tr><td rowspan="6">D11 数据安全和加密</td><td rowspan="5">11.1 概述</td><td>11.1.5 数据安全架构</td><td>应用架构影响数据安全。云提供商提供的功能可以减少攻击面，但确保要求强大的元结构 安全性</td><td>132</td></tr>
<tr><td>11.1.6 监控、审计和告警</td><td>确保将您的日志存储在安全的位置，如专用日志记录帐户。</td><td>133</td></tr>
<tr><td rowspan="2">11.1.7 其他数据安全控制</td><td>数据丢失防护（CASB(云访问和安全代理)、云提供商功能）</td><td>133</td></tr>
<tr><td>数据屏蔽和测试数据生成（测试数据生成、动态屏蔽）</td><td>134</td></tr>
<tr><td>11.1.8 执行声明周期管理安全</td><td>管理数据位置/驻留、确保合规性、备份和业务连续性</td><td>134</td></tr>
<tr><td>11.2 建议</td><td></td><td></td><td>134</td></tr>
<tr><td rowspan="5">D12 身份、授权和访问管理</td><td>12.0 介绍</td><td></td><td>联邦</td><td>136</td></tr>
<tr><td></td><td>12.0.1 云上IAM的差异</td><td>将某种形式的实体(人、系统、代码 等)映射到与各种相关联的可验证身份属性(可以根据当前情况改变)，然后根据授权决定他们 能做什么或不能做什么。</td><td>136</td></tr>
<tr><td rowspan="3">12.1 概述</td><td></td><td>实体、身份、标识符、属性、人物角色、角色、认证、多因素认证(MFA)、访问控制、授权、权利、联邦身份管理、授权源、身份提供者、依赖方</td><td>137</td></tr>
<tr><td>12.1.1 云计算的IAM标准</td><td>安全鉴别标记语言(SAML)2.0、OAuth、OpenID、可扩展访问控制标记语言(XACML)、跨域身份管理系统(SCIM)</td><td>139</td></tr>
<tr><td>12.1.2 管理云计算的用户和身份</td><td>Free-form，Hub and Spoke</td><td>142</td></tr>
</table>