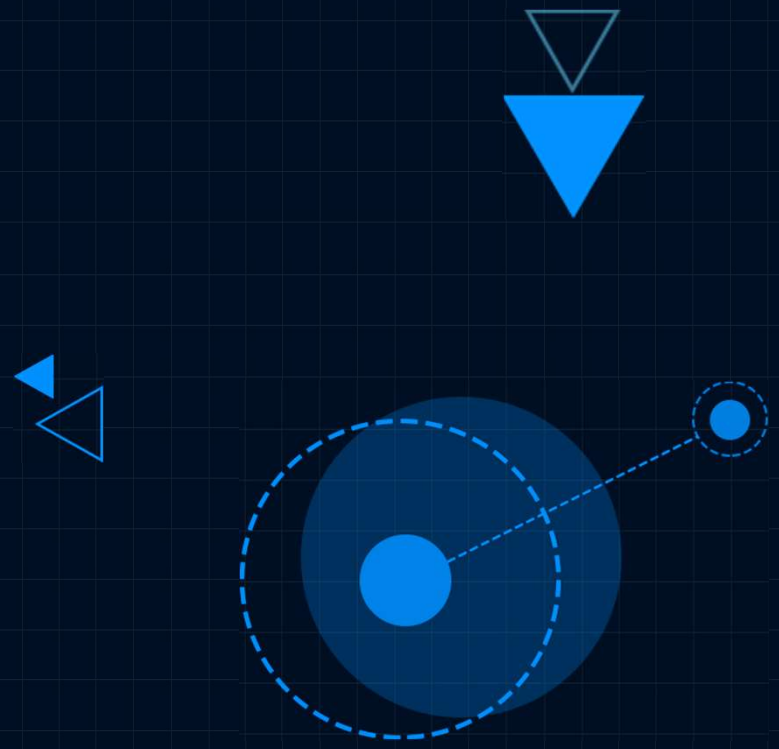
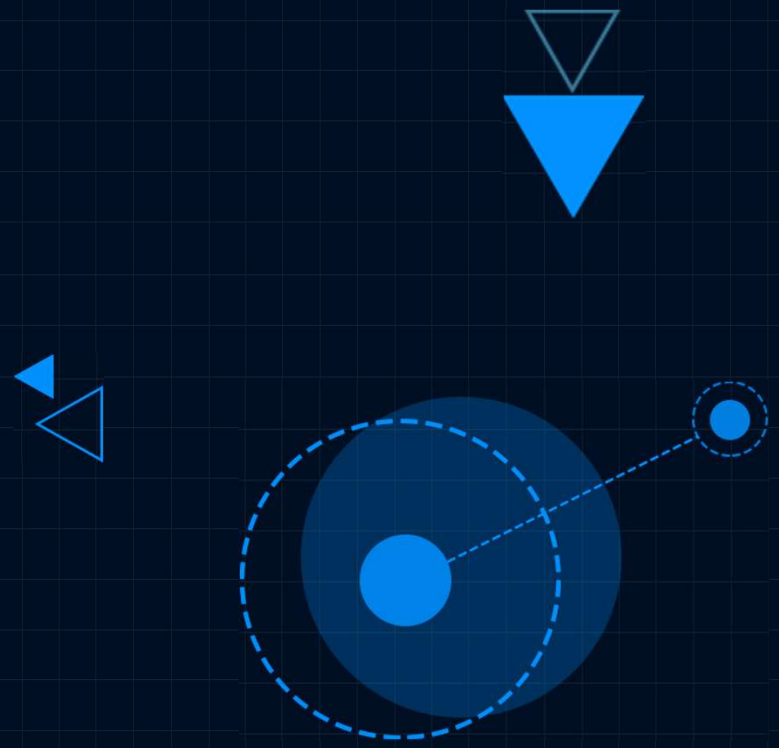
云操作系统的等保与CIS基础安全加固

李艺林

阿里云操作系统团队高级安全工程师



0.背景



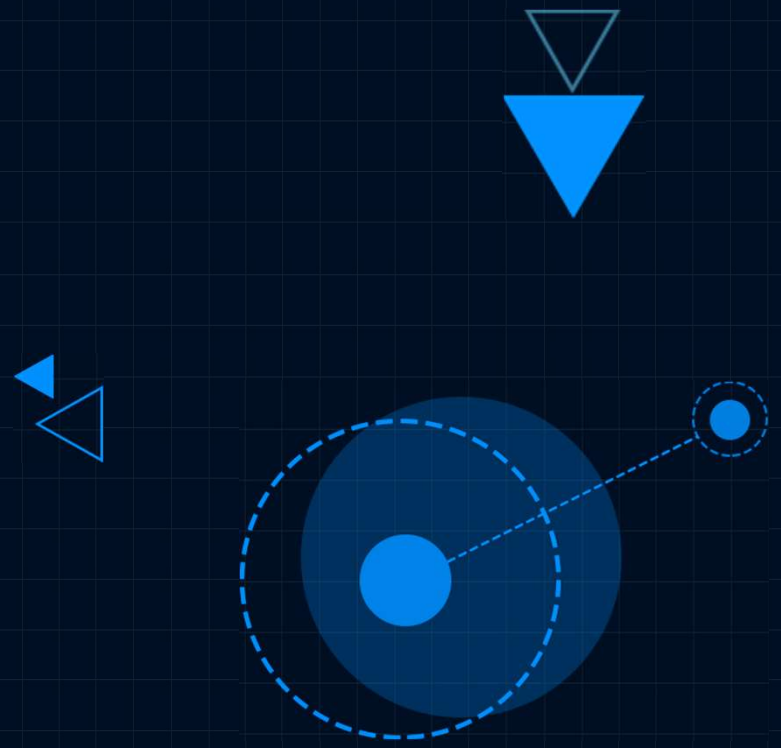
等保与CIS

	等保	CIS (Center for Internet Security)
介绍	我国实行的网络安全等级保护制度	美国知名的网络安全组织
使用范围	中国大陆（主要是银行等国企）	港澳台地区以及国外
加固条目	加固条目相对较少（几十条）	加固条目相对较多（几百条）
安全等级	等保一级/二级/三级等	Level 1/Level 2等
计分规则	没有明显的计分/不计分的分类	有明显的计分/不计分的分类

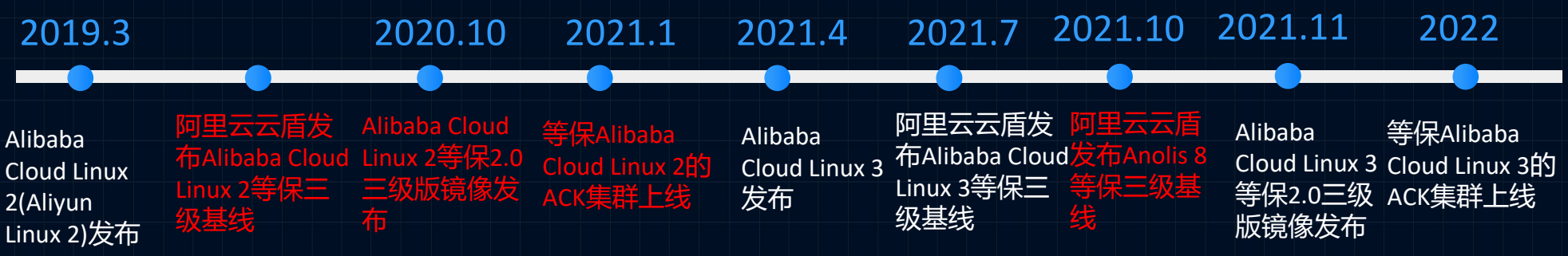
Alibaba Cloud Linux 操作系统

- Alibaba Cloud Linux 2（https://help.aliyun.com/document_detail/154950.html）：兼容Centos 7生态，是阿里云官方操作系统镜像和ACK的首选默认镜像
- Alibaba Cloud Linux 3（https://help.aliyun.com/document_detail/212630.html）：兼容Centos 8生态，目前已经发布LTS版本

1.阿里云操作系统等保安全加固

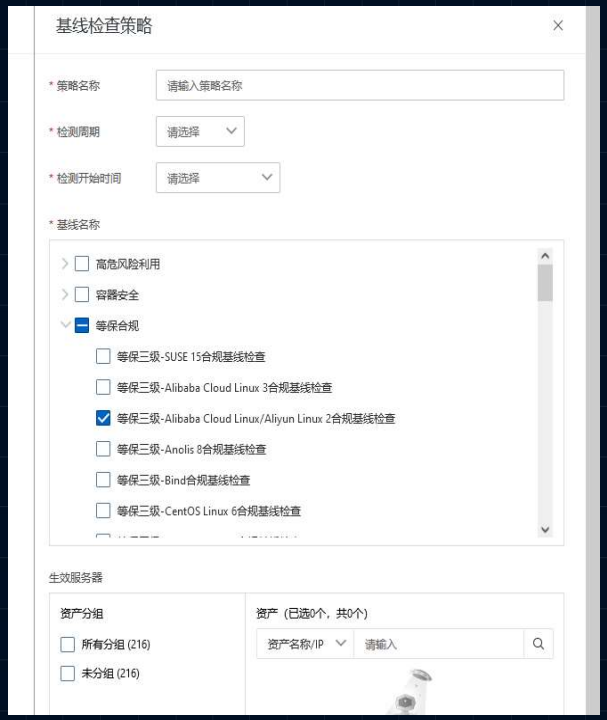


Alibaba Cloud Linux 等保 Milestone



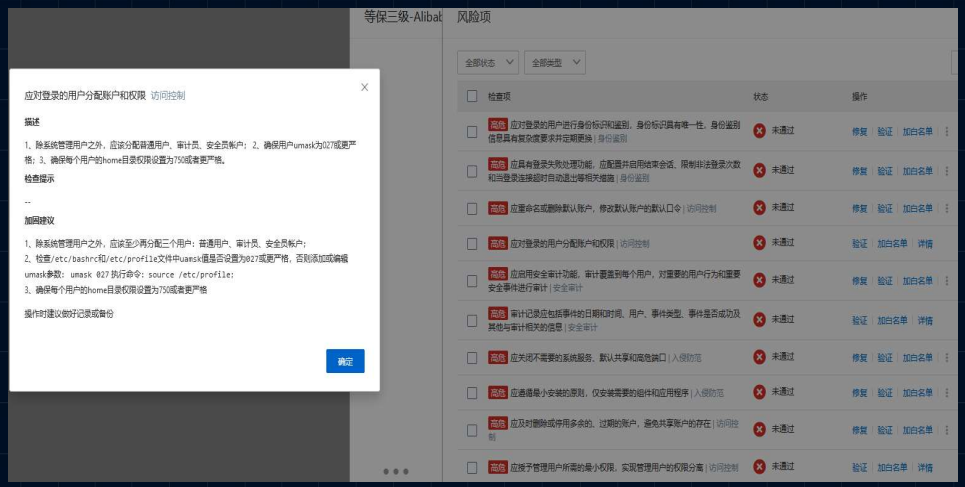
Alibaba Cloud Linux 等保基线

- 阿里云安全中心提供等保三级等基线检查（https://help.aliyun.com/document_detail/42306.htm）：包括Alibaba Cloud Linux 2/3 、Anolis 8、centos等多种操作系统
- Alibaba Cloud Linux 2 检查项包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码攻击五个方面19项，每一项又包含1-7个小项，总共40余个小项：https://help.aliyun.com/document_detail/290803.htm
- 配置Alibaba Cloud Linux 2等保2.0三级基线（https://help.aliyun.com/document_detail/290805.htm）：支持手动和自动扫描。



Alibaba Cloud Linux 等保镜像

- 阿里云安全中心的扫描基线：对系统未通过的扫描项提供修复建议：但是不利于产品化，增加了人工成本等。
- Alibaba Cloud Linux 2等保2.0三级版镜像（https://help.aliyun.com/document_detail/186245.html）：还提供FAQ文档
  - 节省成本：完全免费提供使用的，但需要支付其他资源产生的费用，如vCPU、内存、存储、公网带宽和快照等
  - 节省时间：云安全中心提供基线检查策略，系统将自动判断实例是否达到了等保合规的要求
  - 节省人力：通过已完成等保加固的自定义镜像，批量部署（https://help.aliyun.com/document_detail/197719.htm）

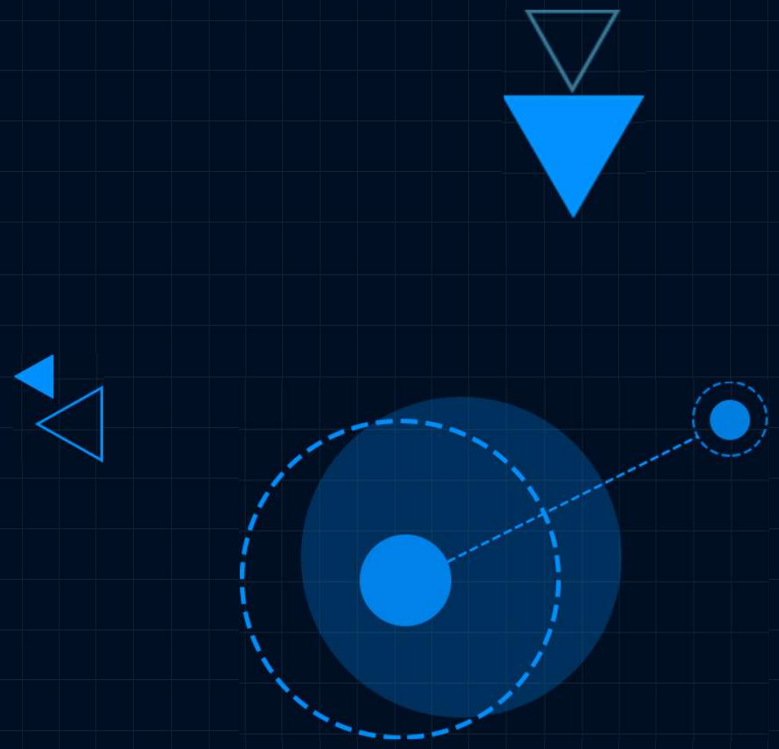



```
欢迎使用 Alibaba Cloud Linux 2 等保合规镜像
1.概述
   Alibaba Cloud Linux 2 等保合规镜像是基于 Alibaba Cloud Linux 2 官方镜像，根据《GB/T22239-2019信息安全技术网络安全等级保护基本要求》进行等保加固的镜像，用户使用本镜像无需额外配置即可满足大部分等保合规要求：
    （1）身份鉴别
    （2）访问控制
    （3）安全审计
    （4）入侵防范
    （5）恶意代码防范
2.使用指南
   按照《GB/T22239-2019信息安全技术网络安全等级保护基本要求》，部分配置需要用户手动执行命令进行配置。用户可以通过 root 账户登录系统后，执行/root/cybersecurity.sh 脚本来实现这类加固。
```

ACK等保集群

- ACK集群：https://help.aliyun.com/document_detail/86987.html
- Alibaba Cloud Linux等保集群：https://help.aliyun.com/document_detail/196148.html
- Alibaba Cloud Linux等保集群优势：
  - Alibaba Cloud Linux 2是ACK的默认操作系统镜像，能够提高ACK集群的安全水位。
  - 同时支持Pro版本、标准版、专有版三种ACK集群形态。
  - 通过ACK集群相关的CI/CD
  - 在ACK集群购买时，如果勾选等保加固，则对集群所有Alibaba Cloud Linux节点（包括master节点）进行等保加固，使得整个集群所有节点通过等保要求。
  - 也可以采用阿里云中心的基线扫描进行检测。

2.阿里云操作系统CIS安全加固



Alibaba Cloud Linux CIS Milestone

2019.3
Alibaba Cloud Linux 2(Aliyun Linux 2)发布

2019.8
Alibaba Cloud Linux 2 CIS认证完成（发布benchmarks、build kit、CIS-CAT）

2021.3
ACK完成k8s CIS认证完成（国内首家云厂商）

2021.4
Alibaba Cloud Linux 3发布

2021.6
Alibaba Cloud Linux 2 CIS加固集群上线

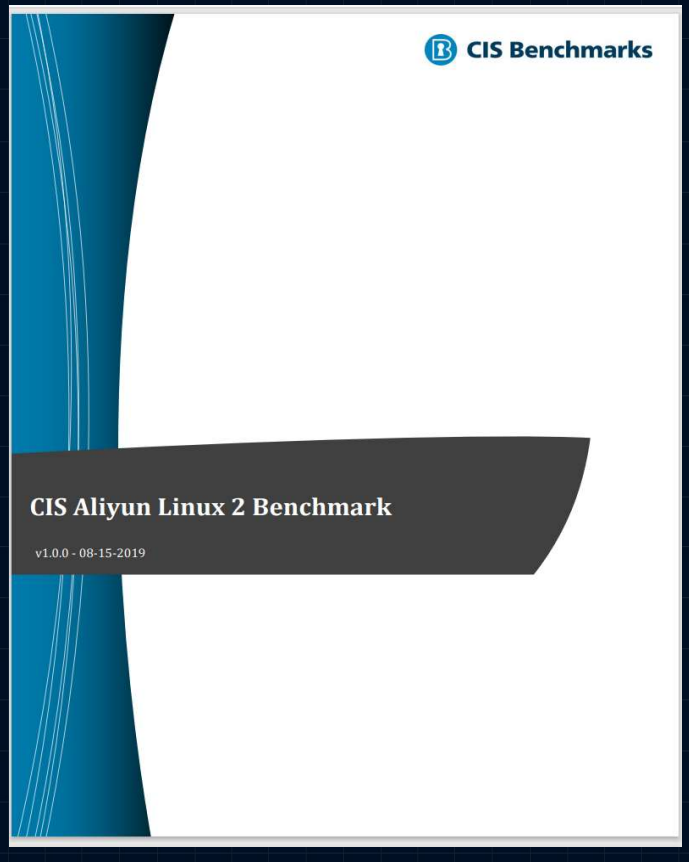
2022.1
Alibaba Cloud Linux 3 CIS认证完成（发布benchmarks、build kit、CIS-CAT）

2022.3
Alibaba Cloud Linux 3 CIS加固集群上线

2022.5
Alibaba Cloud Linux CIS加固镜像

Alibaba Cloud Linux 2 CIS benchmark

- CIS benchmarks(https://workbench.cisecurity.org/): Centos、 Ubuntu、 Amazon等操作系统完成了CIS认证，Alibaba Cloud Linux是国内第一家完成CIS认证的操作系统厂商。
- Alibaba Cloud Linux 2 CIS benchmark（注册后免费下载）：
  - 包含Initial Setup、 Services、 Network Configuration、 Logging and Auditing、 Access, Authentication and Authorization、 System Maintenance六大方面共204项，每一项又包含描述、如何修复、影响、检测等内容，非常详细。
  - 从安全等级上分为level 1和level 2，从计分规则上分为Scored和Not Scored。这四类具体：Level 1 Scored（共145项）、Level 1 Not Scored（共21项）、Level 2 Scored（共33项）、Level 2 Not Scored（共3项）



- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

Scored

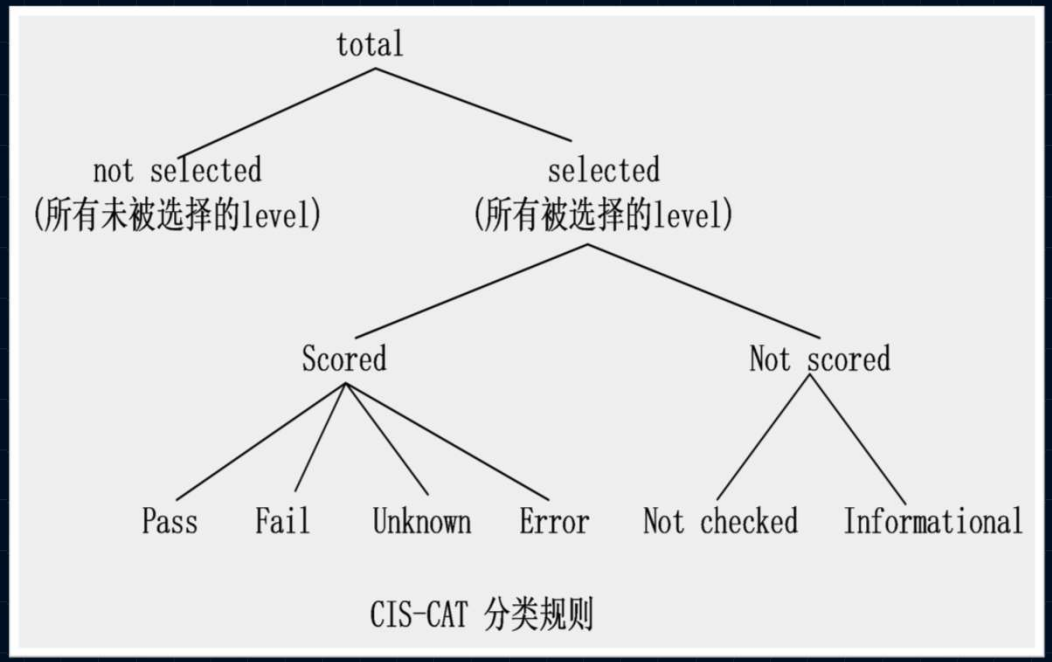
Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

CIS-CAT 扫描工具

- CIS-CAT扫描工具：
  - Lite版（免费但只支持几个桌面操作系统）和 Pro版（收费）
  - 依赖于java
  - 通过参数来选择对应的操作系统（-b参数）以及对应的安全等级(-p参数)
  - 扫描结果解释：https://ccpa-docs.readthedocs.io/en/latest/User%20Guide%20-%20Assessor/



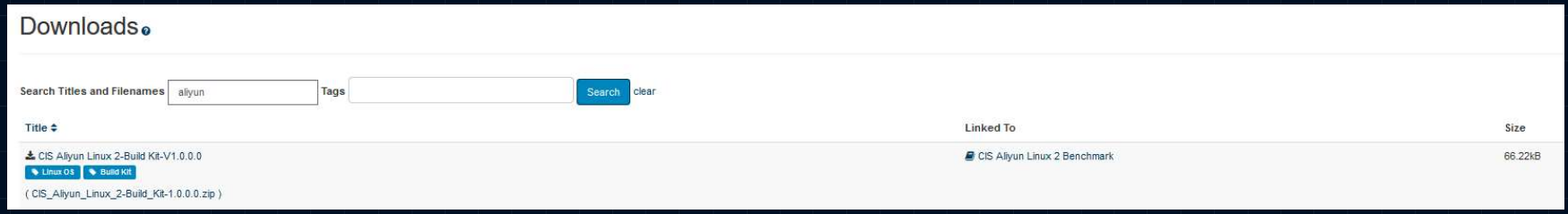
CIS-CAT 分类规则

CIS level 1扫描结果

```
--------------------------------------------------------------------------------
***** Assessment Results Summary *****
--------------------------------------------------------------------------------

   Total # of Results: 204
Total Scored Results: 145
          Total Pass: 73
          Total Fail: 65
         Total Error: 7
       Total Unknown: 0
Total Not Applicable: 0
    Total Not Checked: 11
   Total Not Selected: 36
  Total Informational: 12
--------------------------------------------------------------------------------
***** Assessment Scoring *****
--------------------------------------------------------------------------------

        Score Earned: 73.0
    Maximum Available: 145.0
               Total: 50.34%
--------------------------------------------------------------------------------


- Generating Checklist Results...

Ending Assessment - Date & Time: 03-07-2021 19:16:20
Total Assessment Time: 55 seconds
```

Alibaba Cloud Linux CIS build kit

- Alibaba Cloud Linux 2 CIS build kit：
  - 对CIS会员可见：https://workbench.cisecurity.org/files?q=aliyun&tags=
  - 灵活：几乎每个项有一个修复脚本，脚本文件以benchmark的编号命名，可以通过配置文件来选择要对系统进行哪些加固（其它操作系统几乎没有这一点）。
  - 可读：提供README说明哪些项需要用户自己去手动加固等。




```
$tree .
.
├── CIS_Aliyun_Linux_2_Benchmark.config
├── CIS_Aliyun_Linux_2_Benchmarks
│   ├── 1.1.10.sh
│   ├── 1.1.11.sh
│   ├── 1.1.12.sh
│   ├── 1.1.13.sh
│   ├── 1.1.14.sh
│   ├── 1.1.15.sh
│   ├── 1.1.16.sh
│   ├── 1.1.17.sh
│   ├── 1.1.1.sh
│   ├── 1.1.3.sh
│   ├── 1.1.4.sh
│   ├── 1.1.5.sh
│   ├── 1.1.6.sh
│   ├── 1.1.7.sh
│   ├── 1.1.8.sh
│   ├── 1.1.9.sh
│   ├── 1.2.3.sh
│   ├── 1.3.1.sh
│   ├── 1.3.2.sh
│   ├── 1.4.1.sh
│   ├── 1.4.2.sh
│   ├── 1.5.1.sh
│   ├── 1.5.2.sh
│   ├── 1.5.3.sh
│   ├── 1.6.1.1.sh
│   ├── 6.1.2.sh
│   ├── 6.1.3.sh
│   ├── 6.1.4.sh
│   ├── 6.1.5.sh
│   ├── 6.1.6.sh
│   ├── 6.1.7.sh
│   ├── 6.1.8.sh
│   ├── 6.1.9.sh
│   ├── 6.2.10.sh
│   ├── 6.2.11.sh
│   ├── 6.2.12.sh
│   ├── 6.2.13.sh
│   ├── 6.2.14.sh
│   ├── 6.2.15.sh
│   ├── 6.2.16.sh
│   ├── 6.2.17.sh
│   ├── 6.2.18.sh
│   ├── 6.2.19.sh
│   ├── 6.2.1.sh
│   ├── 6.2.2.sh
│   ├── 6.2.3.sh
│   ├── 6.2.4.sh
│   ├── 6.2.5.sh
│   ├── 6.2.6.sh
│   ├── 6.2.7.sh
│   ├── 6.2.8.sh
│   └── 6.2.9.sh
├── Makefile
├── README
└── run_remediation_kit.sh

1 directory, 188 files
```

```
$cat README
This archive contains shell scripts for configuring Aliyun Linux 2 in compliance with the CIS Aliyun Linux 2 benchmark v1.0.0.  It was tested against Aliyun Linux
2 as assessed by CIS-CAT v4.0.8.

To execute the script pass a single parameter for the profile desired:
#sh run_remediation_kit.sh test.config

where the file "test.config" includes the benchmark items (the numbers like 1.1.1,  2.1.1.1) split by empty lines.

If no parameter is passed the script will default to "CIS_Aliyun_Linux_2_Benchmark.config" which includes all the benchmark items parsed from CIS Aliyun Linux 2 be
nchmark v1.0.0.

In addition to non CIS-CAT assessed items, the following are not configured by this script:

1.1.2 - 1.1.17
System partitioning must be completed manually.

2.1.15 Ensure mail transfer agent is configured for local-only mode
Remediation depends on MTA in use.

3.3.3 Ensure /etc/hosts.deny is configured
Automated configuration may lockout administration.

3.5.1.1 - 3.5.2.2
Automated configuration may lockout administration.

4.2.1.1 - 4.2.1.4
Log server configuration should be configured by hand to prevent misconfiguration.

5.2.3  Ensure permissions on SSH private host key files are configured
The GID of ssh_keys may have changed from 998 to 997, should be checked manually.

5.2.10 Ensure SSH root login is disabled (Scored)
Please create other users to login before exec this script.

5.2.18 Ensure SSH access is limited
Automated configuration may lockout administration.
```

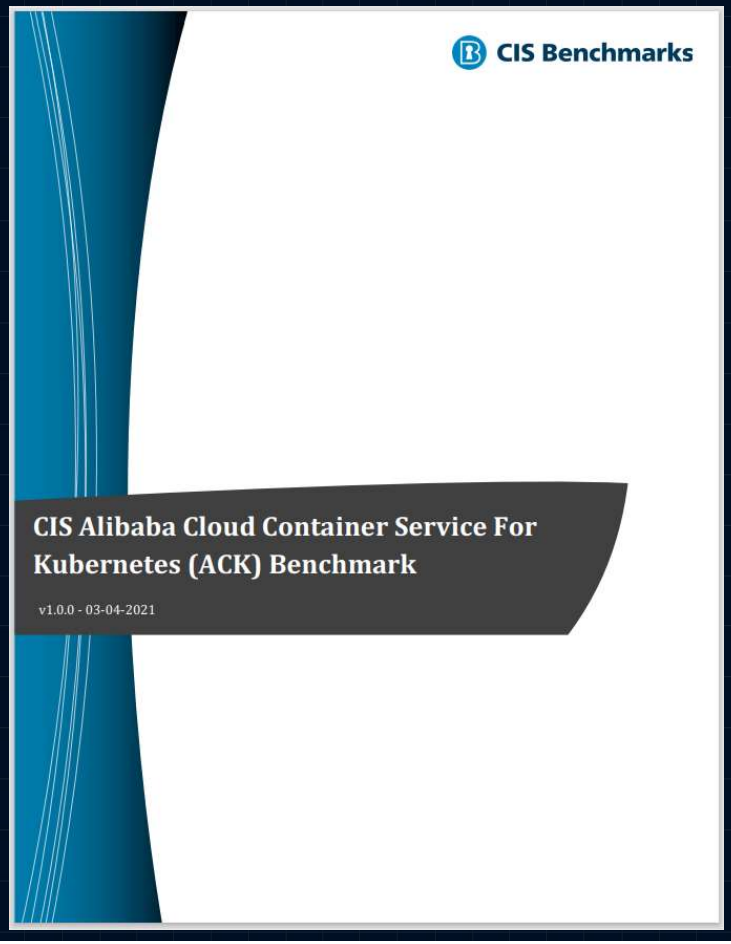
ACK CIS 加固集群

- Alibaba Cloud Linux CIS集群：https://help.aliyun.com/document_detail/223744.html
- Alibaba Cloud Linux CIS集群优势：
  - Alibaba Cloud Linux 2是ACK的默认操作系统镜像，能够提高ACK集群的安全水位。
  - 同时支持Pro版本、标准版、专有版三种ACK集群形态。
  - 通过ACK集群相关的CI/CD
  - 在ACK集群购买时，如果勾选CIS加固，对集群所有Alibaba Cloud Linux节点（包括master节点）进行CIS level 1加固（CIS level 2未加固），使得整个集群所有节点通过CIS level 1 Scored项128项，88%以上，未通过的加固项（需要用户加固等）给出理由和指南。
  - 也可以采用CIS中心提供的CIS-CAT进行扫描验证。


```
------------------------------------------------------------------------------
***** Assessment Results Summary *****
------------------------------------------------------------------------------
   Total # of Results: 204
 Total Scored Results: 145
           Total Pass: 128
           Total Fail: 17
          Total Error: 0
        Total Unknown: 0
 Total Not Applicable: 0
    Total Not Checked: 11
   Total Not Selected: 36
  Total Informational: 12
------------------------------------------------------------------------------
***** Assessment Scoring *****
------------------------------------------------------------------------------
         Score Earned: 128.0
    Maximum Available: 145.0
                Total: 88.28%
------------------------------------------------------------------------------
```

ACK CIS benchmark

- CIS benchmarks(https://workbench.cisecurity.org/): AWS、aliyun等云厂商完成了CIS认证，阿里云ACK是国内第一家完成k8s CIS认证的云厂商。
- ACK CIS benchmark（注册后免费下载）：
  - 包含Control Plane Components、etcd、Control Plane Configuration、Worker Nodes、 Policies、Managed services六大方面几百项，每一项又包含描述、如何修复、影响、检测等内容，非常详细。
  - 从安全等级上分为level 1和level 2，每个level又分为Master Node和Worker Node。
  - 从计分规则上分为Automated和Manual。



Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Master Node**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

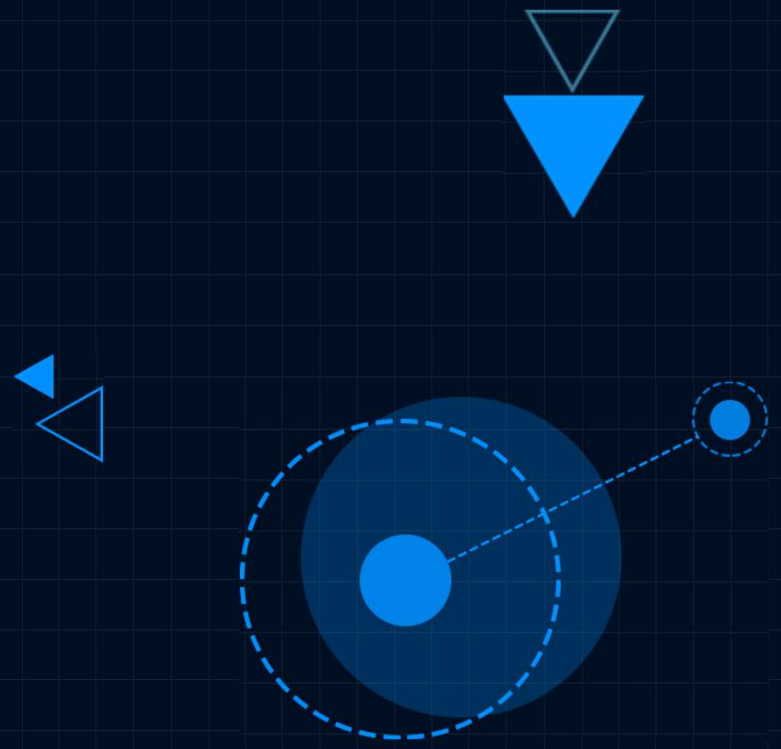
- **Level 2 - Master Node**
- **Level 1 - Worker Node**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2 - Worker Node**

3.总结与展望



总结与展望

- 总结

  围绕Alibaba Cloud Linux 2/3 操作系统介绍阿里云在等保与CIS方面的一些工作（包括部分规划）

- 展望

  1. 结合Alibaba Cloud Linux 2/3的上游操作系统Anolis os 7/8（https://openanolis.cn/）继续开展等保/CIS的基础安全加固工作（包括创建SIG等）

  2. 在其它操作系统安全领域（商密、机密计算等）开展更多的工作, 使得操作系统更加安全。

     （1）Anolis os 全栈商密镜像（Anolis OS ShangMi Beta）：https://openanolis.cn/download

     （2）机密计算：围绕Intel SGX/TDX展开的容器运行时Inclavare Containers（https://github.com/alibaba/inclavare-containers）

Thanks_