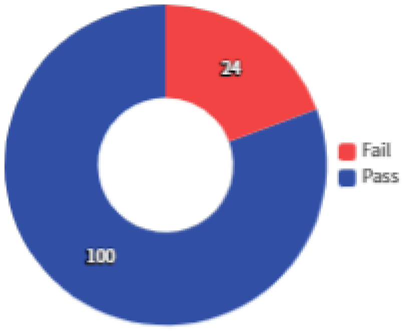
Scan Report

01. Summary

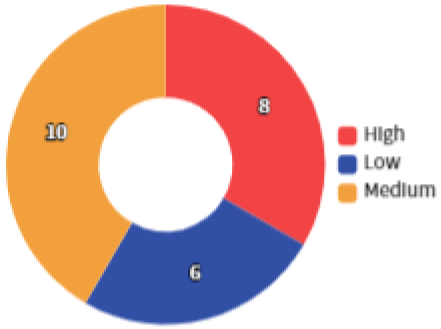
Scan Date	22.12.17	**Account**	account
Cloud Service Provider	Ncloud	**Scan Target**	InitCloud.zip

Total Scanned Rules	Passed Rules	Failed Rules
124	100	24

Scan Results



Failure Status by Severity



Failure Status by Resource

access control group	**server**	**network acl**	**auto scaling**	**nks cluster**
2	1	3	1	1
lb	**nas_volume**	**key**	**route**	**subnet**
4	2	4	6	0

Failure Status by ISMS-P

2.5 인증 및 권한관리	11	**2.10 시스템 및 서비스 보안관리**	1
2.6 접근통제	1	**2.11 사고 예방 및 대응**	2
2.7 암호화 적용	4	**2.12 재해복구**	5
2.9 시스템 및 서비스 운영관리	7	**Total**	31

Failure Status by Security Threat

AUDIT AND ACCOUNTABILIY	**ACCESS CONTROL**	**MEDIA PROTECTION**	**SYSTEM AND COMMUNICATIONS PROTECTION**	**SYSTEM AND INFORMATION INTEGRITY**
2	2	2	4	3
INCIDENT RESPONSE	**IDENTIFICATION AND AUTHENTICATION**	**CONFIGURATION MANAGEMENT**	**CONTINGENCY PLANNING**	**PERFORMANCE IMPROVEMENTS**
3	2	1	5	1

IaC score : **60.7**

Score is based on severity

02. Scan Details

RuleID	Policy	Severity	ScanResult	Solution	ControlName	Article
CKV_NCP_2	Ensure every access control groups rule has a description	Low	F	링크	isms-p	2.10.2
CKV_NCP_3	Ensure no security group rules allow outbound traffic to 0.0.0.0/0	High	F	링크	isms-p	2.6.1
CKV_NCP_6	Ensure Server instance is encrypted	High	F	링크	isms-p	2.6.2 2.7.1
CKV_NCP_8	Ensure no NACL allow inbound from 0.0.0.0:0 to port 20	High	F	링크	isms-p	2.6.1 2.10.9 2.6.7
CKV_NCP_9	Ensure no NACL allow inbound from 0.0.0.0:0 to port 21	High	F	링크	isms-p	2.6.1 2.10.9 2.6.7
CKV_NCP_10	Ensure no NACL allow inbound from 0.0.0.0:0 to port 22	High	F	링크	isms-p	2.6.1 2.10.9 2.6.7
CKV_NCP_18	Ensure that auto Scaling groups that are associated with a load balancer, are using Load Balancing health checks.	Low	F	링크	isms-p	2.9.2 2.10.2
CKV_NCP_19	Ensure NKS public endpoint disabled.	High	F	링크	isms-p	2.6.1 2.6.2 2.6.7 2.10.9
CKV_NCP_1	Ensure HTTP HTTPS Target group defines Healthcheck.	High	P	링크	isms-p	2.9.2 2.10.2
CKV_NCP_3	Ensure no security group rules allow outbound traffic to 0.0.0.0/0	High	P	링크	isms-p	2.6.1
CKV_NCP_6	Ensure Server instance is encrypted	High	P	링크	isms-p	2.6.2 2.7.1
CKV_NCP_6	Ensure Server instance is encrypted	High	P	링크	isms-p	2.6.2 2.7.1
CKV_NCP_6	Ensure Server instance is encrypted	High	P	링크	isms-p	2.6.2 2.7.1
CKV_NCP_11	Ensure no NACL allow inbound from 0.0.0.0:0 to port 3389	High	P	링크	isms-p	2.6.1 2.10.9 2.6.7
CKV_NCP_11	Ensure no NACL allow inbound from 0.0.0.0:0 to port 3389	High	P	링크	isms-p	2.6.1 2.10.9 2.6.7
CKV_NCP_13	Ensure that load balancer is using TLS 1.2	High	P	링크	isms-p	2.10.5 2.10.9 2.7.1
CKV_NCP_14	Ensure NAS volume is encrypted.	High	P	링크	isms-p	2.6.2 2.7.1
CKV_NCP_15	Ensure LB protocol is HTTPS.	High	P	링크	isms-p	2.10.5 2.10.9 2.7.1
CKV_NCP_18	Ensure that auto Scaling groups that are associated with a load balancer, are using Load Balancing health checks.	Low	P	링크	isms-p	2.9.2 2.10.2

CKV_NCP_8

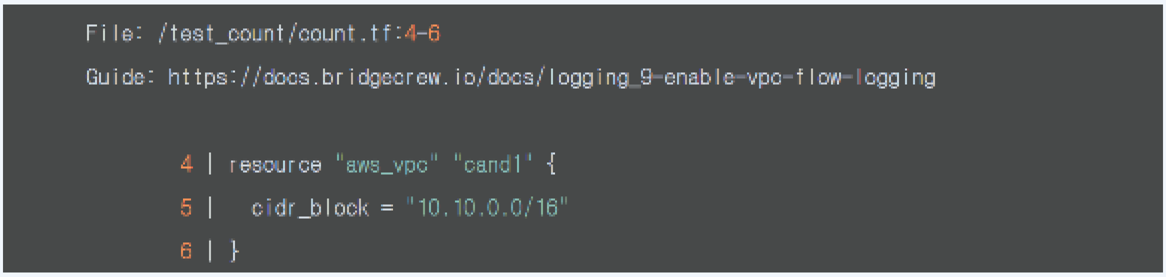
Result	FAIL	Severity	High

Rule Description

description	Ensure no NACL allow inbound from 0.0.0.0:0 to port 20		
type	SYSTEM AND COMMUNICATIONS PROTECTION, SYSTEM AND INFORMATION INTEGRITY	**problematic location**	file name: main.tf line: 5-10
resource	ncloud_access_control_group	**resource name**	test_acg
compliance	isms-p	**article**	2.6.1, 2.6.7, 2.10.9

Drawback

Problematic code



```
      File: /test_count/count.tf:4-6
      Guide: https://docs.bridgecrew.io/docs/logging_9-enable-vpc-flow-logging

              4 | resource "aws_vpc" "cand1" {
              5 |   cidr_block = "10.10.0.0/16"
              6 | }
```

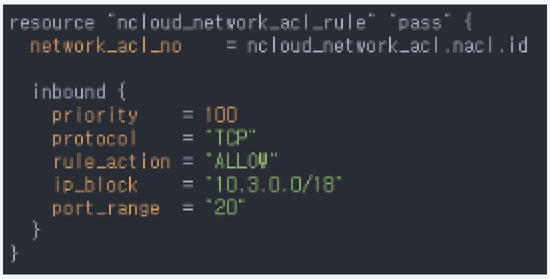
Unfulfilled Compliance

isms-p	details
2.6.1	Access to all IP blocks to the port should not be possible to prevent unauthorized access to the network.
2.6.7	Since major information systems need to control unnecessary external Internet access, all IPs should not have internal access.
2.10.9	To protect the system from malware, all IPs should not be able to access it internally.

Possible impact

Public access to remote server management ports can increase resource attack areas and unnecessarily increase the risk of resource corruption.

Solution



```
resource "ncloud_network_acl_rule" "pass" {
  network_acl_no     = ncloud_network_acl.nacl.id

  inbound {
    priority    = 100
    protocol    = "TCP"
    rule_action = "ALLOW"
    ip_block    = "10.3.0.0/18"
    port_range  = "20"
  }
}
```

In the inbound rule of ncloud_network_acl_rule, if the port number is 20, ip_block should be set to a specific cidr block instead of 0.0.0.0/0.