RONIN LOGGING

OVERVIEW

All versions of the RONIN platform (RONIN Core and RONIN Isolate) log data that can be used for compliance and security monitoring, as well as performance monitoring and optimization. RONIN logging is detailed and is designed to be supplemented by AWS services, or third party log processing tools (e.g. Splunk, Sumo Logic), to log and monitor events. This configurability is necessary as customer needs vary significantly, and one size does not fit all.

There are three sources of RONIN logging data:

- The **RONIN User Interface** (UI). All UI actions are logged.
- **AWS CloudTrail**. AWS CloudTrail is not configured by default except for RONIN Isolate builds. It logs actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.
- **Amazon CloudWatch**. Amazon CloudWatch collects monitoring and operational data. Amazon CloudWatch is configured by default to log performance data for machines and clusters created within RONIN. If desired, this data can be used by system administrators to identify machines that are used inefficiently and make recommendations on how to save money.

Depending on your security and compliance needs, you can;

- Augment the default logging by configuring AWS CloudTrail and Amazon CloudWatch.
- Configure Amazon CloudWatch to detect anomalous behavior in your environments, set alarms, take automated actions, troubleshoot issues, and discover insights to keep your applications.
- Configure third party log analysis tools, or write custom scripts, to detect anomalous behavior or take automated actions.

We describe default logging from the above three sources in the following sections.

RONIN UI LOGS

The RONIN UI logs every action taken by a user and important outcomes, together with the remote IP address, RONIN User ID, Session Log, and Server Log. These four data elements are written out in a JSON structure. The specific RONIN actions that are logged, Session Log and Server Log are described in more detail below. See Appendix A for a complete RONIN UI log entry for the CREATE_MACHINE operation, as an example.

RONIN UI LOGGED ACTIONS

RONIN logs the actions provided in the table below, and where specified, additional information that is required for the action.

Action Logged	Additional Parameters
LOGGED_OUT	
ACCESS_LOGIN_SCREEN	
USER_LOGGED_IN_SUCCESS	
USER_LOGGED_IN_SUCCESS_OAUTH	
USER_FAILED_LOGIN_OAUTH	
COGNITO_ACCESS_TOKEN_NOT_FOUND	
COGNITO_REFRESH_TOKEN_NOT_FOUND	
COGNITO_TOKEN_EXPIRED	
CLUSTER_STARTED	$instance [InstanceID from the cluster master node]
CLUSTER_STOPPED	$instance [InstanceID from the cluster master node]
CREATE_CLUSTER	$tagsArr [All the ec2 tags for this resource]
DELETE_CLUSTER	$stackName [Full name of the cluster stack]
ATTACH_VOLUME	$tagsArr [All the ec2 tags for this resource]

PACKAGE_CREATED	$result [Array of status, result dump of webservice action]
CREATE_VOLUME	$log = [$name, $size, $storageType, $snapshot];
CREATE_MACHINE	Instance dump of what is returned from successful webservice call
DELETE_VOLUME	$volumeId
DELETE_MACHINE_KEY	$keyName
PACKAGE_CREATED	$result [Array of status, result dump of webservice action]
PACKAGE_DEREGISTERED	$amiId
DETACH_VOLUME	$log = [$instance, $volume, $device];
NEW_MACHINE_KEY	$keyName
MACHINE_STARTED	$InstanceId
MACHINE_STOPPED	$InstanceId
TERMINATE_MACHINE	$result [Array of status, result dump of webservice action]
DELETE_BUCKET_KEY	$keyId
CREATE_BUCKET_KEY_ADMIN (ADMIN = Read/Write)	$accessKey
CREATE_BUCKET_KEY_READ (READ = Read only)	$accessKey
CREATE_BUCKET	$bucketName
DELETE_BUCKET	$bucketName
PASSWORD_RESET	$instanceId
PROJECT_CREATED	RPID USER NAME DESCRIPTION

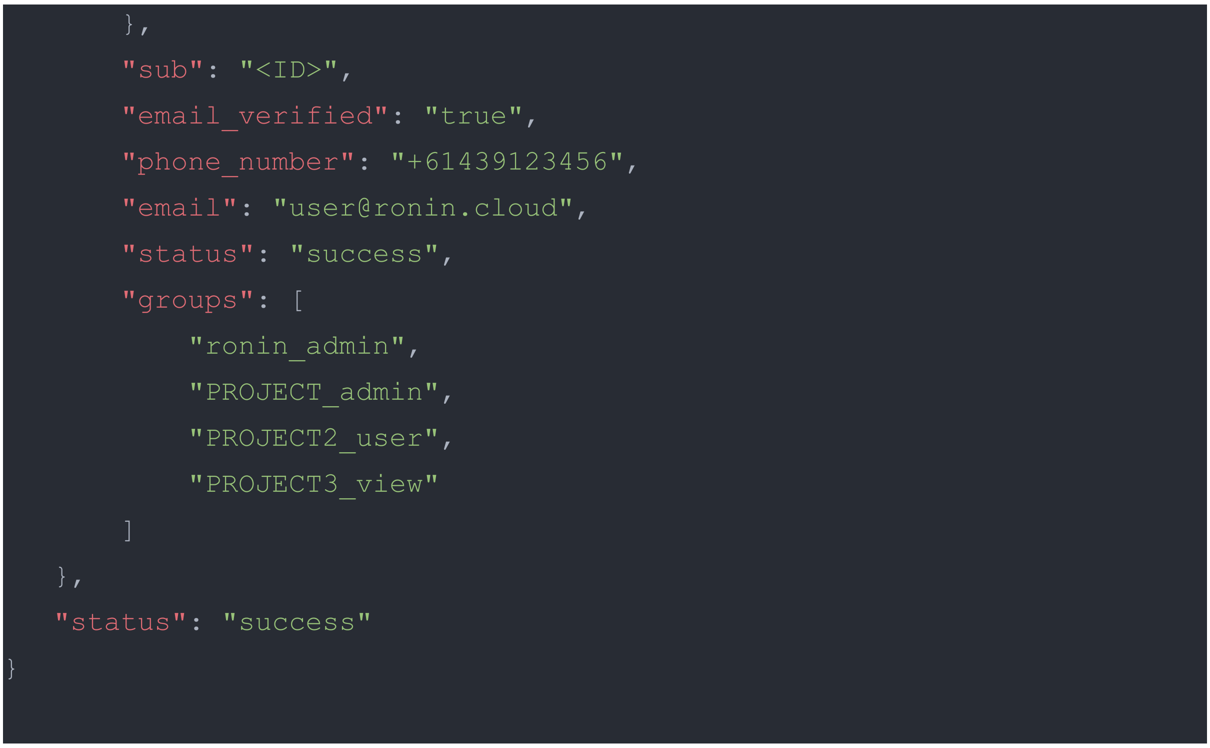
	SUMMARY TAGS STARTDATE ENDDATE BUDGET AUTOPAUSE INVOICEEMAIL BILLINGCODE PURCHASEORDER $array [All admins, users and viewers for the project, what action was triggered for that user (add, remove)]
PROJECT_UPDATED	SAME AS PROJECT_CREATED
PROJECT_PAUSED_ADMIN	$userId of person who paused the project (ronin_admin)
PROJECT_PAUSED	$userId of person who soft paused the project (ronin_admin, ronin_lower_admin or project_admin)
PROJECT_CLOSED	$rpid [Ronin Project ID]
PERMISSION_CHANGE	$array [All admins, users and viewers for the project, what action was triggered for that user (add, remove)]
MACHINE_PERMISSION_CHANGE (isolate installs only)	$assocArray [Bucket name, machine array of all instanceid's]
AVATAR_UPLOADED PACKAGE_UPLOADED PROJECT_UPLOADED	A picture has been uploaded to associate to resource
SMART_SCHEDULE_ON	$machine
SMART_SCHEDULE_OFF	$machine

SESSION LOG

Your session has details of everything related to your RONIN Login.

Below is an example of the JSON log related to a session, here using Cognito.

```
{
    "csrfp_ronin_token": [
        "<TOKEN>"
    ],
    "CREATED": 1629682992,
    "auth": {
        "ChallengeParameters": [],
        "AuthenticationResult": {
            "AccessToken": "<TOKEN>",
            "ExpiresIn": 3600,
            "TokenType": "Bearer",
            "RefreshToken": "<TOKEN>",
            "IdToken": "<TOKEN>"
        },
        "@metadata": {
            "statusCode": 200,
            "effectiveUri":
"https:\/\/cognito-idp.ap-southeast-2.amazonaws.com",
            "headers": {
                "date": "Mon, 23 Aug 2021 01:43:12 GMT",
                "content-type": "application\/x-amz-json-1.1",
                "content-length": "3914",
                "connection": "keep-alive",
                "x-amzn-requestid": "<ID>"
            },
            "transferStats": {
                "http": [
                    []
                ]
            }
        }
    },
    "user": {
        "Username": "user",
        "UserAttributes": [
            {
                "Name": "sub",
                "Value": "<ID>"
            },
            {
                "Name": "email_verified",
                "Value": "true"
            },
            {
                "Name": "phone_number",
                "Value": "+61439123456"
            },
            {
                "Name": "email",
                "Value": "user@ronin.cloud"
            }
        ],
        "UserCreateDate": {
            "date": "2019-05-16 05:57:54.000000",
            "timezone_type": 1,
            "timezone": "+00:00"
        },
        "UserLastModifiedDate": {
            "date": "2021-05-11 01:14:03.000000",
            "timezone_type": 1,
            "timezone": "+00:00"
        },
        "Enabled": true,
        "UserStatus": "CONFIRMED",
        "@metadata": {
            "statusCode": 200,
            "effectiveUri":
"https:\/\/cognito-idp.ap-southeast-2.amazonaws.com",
            "headers": {
                "date": "Mon, 23 Aug 2021 01:43:12 GMT",
                "content-type": "application\/x-amz-json-1.1",
                "content-length": "348",
                "connection": "keep-alive",
                "x-amzn-requestid": "<ID>"
            },
            "transferStats": {
                "http": [
                    []
                ]
            }
```



```
        },
        "sub": "<ID>",
        "email_verified": "true",
        "phone_number": "+61439123456",
        "email": "user@ronin.cloud",
        "status": "success",
        "groups": [
            "ronin_admin",
            "PROJECT_admin",
            "PROJECT2_user",
            "PROJECT3_view"
        ]
    },
    "status": "success"
}
```

SERVER LOG

The PHP server log, a basic dump of the PHP $_SERVER variable, contains important variables such as the remote IP address of the entity viewing the current page, and the authenticated remote user.

The components in this array are described in the PHP manual: https://www.php.net/manual/en/reserved.variables.server.php

AMAZON CLOUDWATCH LOGS

Amazon CloudWatch is configured to monitor performance metrics on RONIN machines and clusters (using the unified CloudWatch agent and AWS Systems Manager [SSM]). The Amazon CloudWatch agent configuration is stored within Parameter Store, a tool in AWS Systems Manager. Parameter store allows you to securely store configuration data and secrets for reusability. SSM will use the configuration stored within Parameter Store to instruct the CloudWatch agent installed on the EC2 instances created by RONIN to use this configuration and start collecting logs.

All machines and clusters receive parameters shown in LINUX MACHINES / CLUSTERS and WINDOWS MACHINES, which are collected by the unified CloudWatch agent. You can modify this by adding or removing parameters being watched in the Parameter stores for Linux machines and clusters (ronin-cw-linux) and for Windows machines (ronin-cw-windows).

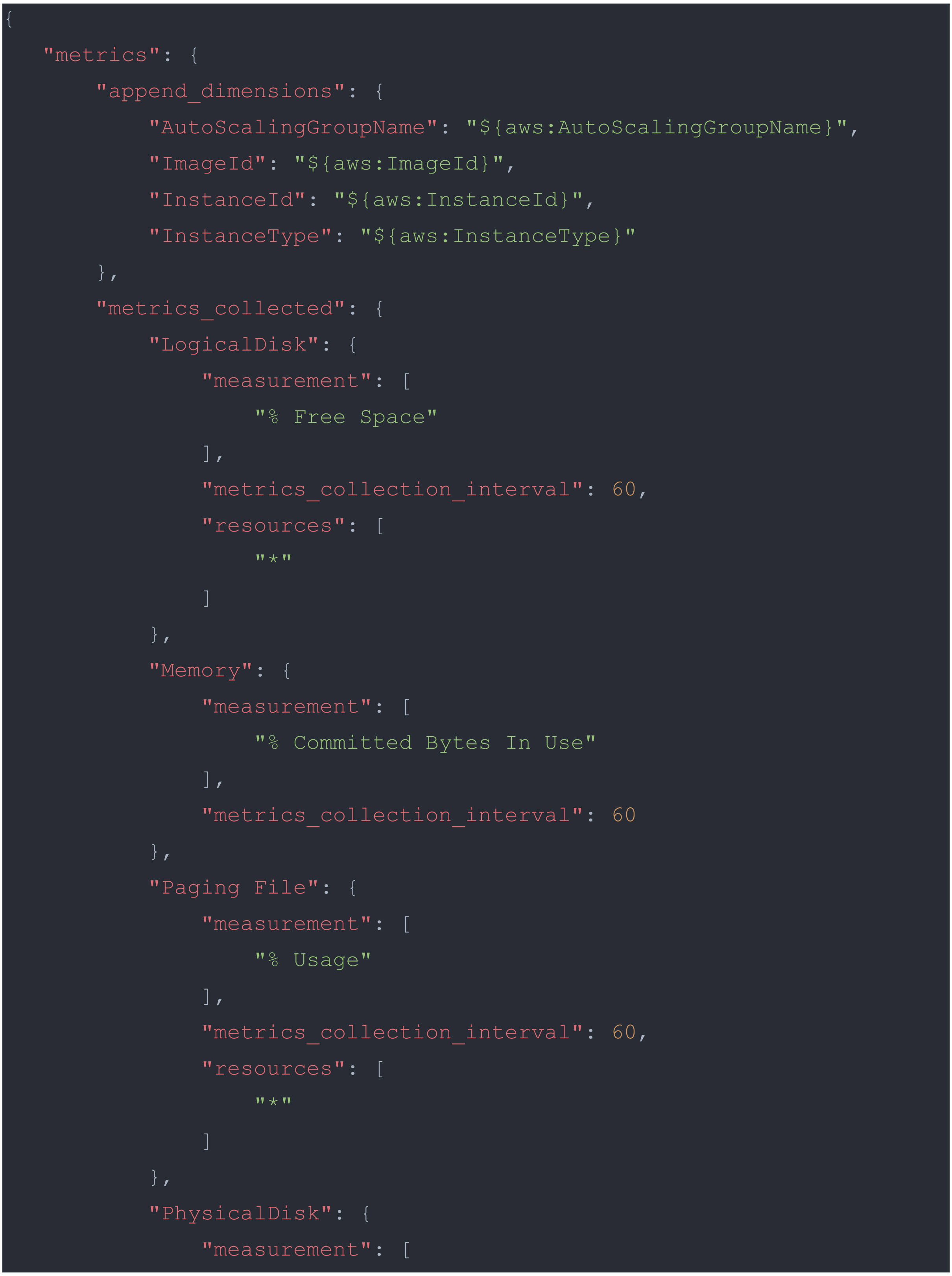
Amazon CloudWatch can also be used to create performance dashboards, analyze and integrate performance metrics with other information, such as audit trails. This allows you to detect anomalous behavior, set alarms, take automated actions and discover insights to optimize performance or cost.

Because different institutions have varying needs for such tooling, and may prefer other solutions for log monitoring and analysis, RONIN has not developed tools for specific analysis of Amazon CloudWatch logs.

LINUX MACHINES / CLUSTERS

```
{
    "metrics": {
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
        "metrics_collected": {
            "cpu": {
                "measurement": [
                    "cpu_usage_idle",
                    "cpu_usage_iowait",
                    "cpu_usage_user",
                    "cpu_usage_system"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ],
                "totalcpu": false
            },
            "disk": {
                "measurement": [
                    "used_percent",
                    "inodes_free"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "diskio": {
                "measurement": [
                    "io_time",
                    "write_bytes",
                    "read_bytes",
                    "writes",
                    "reads"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "mem": {
                "measurement": [
                    "mem_used_percent"
                ],
                "metrics_collection_interval": 60
            },
            "netstat": {
                "measurement": [
                    "tcp_established",
                    "tcp_time_wait"
                ],
                "metrics_collection_interval": 60
            },
            "swap": {
                "measurement": [
                    "swap_used_percent"
                ],
                "metrics_collection_interval": 60
            }
        }
    }
}
```

WINDOWS MACHINES



```
{
    "metrics": {
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
        "metrics_collected": {
            "LogicalDisk": {
                "measurement": [
                    "% Free Space"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "Memory": {
                "measurement": [
                    "% Committed Bytes In Use"
                ],
                "metrics_collection_interval": 60
            },
            "Paging File": {
                "measurement": [
                    "% Usage"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "PhysicalDisk": {
                "measurement": [
                    "% Disk Time",
                    "Disk Write Bytes/sec",
                    "Disk Read Bytes/sec",
                    "Disk Writes/sec",
                    "Disk Reads/sec"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "Processor": {
                "measurement": [
                    "% User Time",
                    "% Idle Time",
                    "% Interrupt Time"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "TCPv4": {
                "measurement": [
                    "Connections Established"
                ],
                "metrics_collection_interval": 60
            },
            "TCPv6": {
                "measurement": [
                    "Connections Established"
                ],
                "metrics_collection_interval": 60
            }
        }
    }
}
```

CLOUDTRAIL LOGS

AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of the AWS account in which RONIN is installed. CloudTrail provides event history of the AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. Specifically, CloudTrail can be used to detect unusual activity in your AWS accounts.

RONIN does not manage your AWS CloudTrail configuration; however, CloudTrail logging is necessary to address HIPAA security controls and full logging is enabled in RONIN Isolate builds. AWS CloudTrail logging can be incorporated into any RONIN build.

Appendix A

Below is an entry for the CREATE_MACHINE log event, with the user_data, session_log and server_log fields converted from strings to json for prettyprinting. In addition, certain fields are altered from their real values.

```
{
  "ts_created": "2022-07-01T14:31:49.822Z",
  "error_code": "ACCESS_LOG",
  "error_message": "CREATE_MACHINE",
  "error_data": {
    "instanceId": {
      "AmiLaunchIndex": 0,
      "ImageId": "ami-0e413a9954960d83a",
      "InstanceId": "i-0ef7cffffffffff",
      "InstanceType": "g4dn.xlarge",
      "KeyName": "RPID:INSPECTOR:batman",
      "LaunchTime": "2022-07-01T14:31:49+00:00",
      "Monitoring": {
        "State": "disabled"
      },
      "Placement": {
        "AvailabilityZone": "ap-southeast-2b",
        "GroupName": "",
        "Tenancy": "default"
      },
      "PrivateDnsName":
"ip-10-0-5-202.ap-southeast-2.compute.internal",
      "PrivateIpAddress": "10.0.5.202",
      "ProductCodes": [],
      "PublicDnsName": "",
      "State": {
        "Code": 0,
        "Name": "pending"
      },
      "StateTransitionReason": "",
      "SubnetId": "subnet-99999999",
      "VpcId": "vpc-19999999c",
      "Architecture": "x86_64",
      "BlockDeviceMappings": [],
      "ClientToken": "88893df2-9b29-4132-88f9-xxxxxxxxx",
      "EbsOptimized": false,
      "EnaSupport": true,
      "Hypervisor": "xen",
      "IamInstanceProfile": {
        "Arn":
"arn:aws:iam::814453012568:instance-profile/ronin-clone",
        "Id": "AIPAILYKRJXRSLNN5637A"
      },
      "NetworkInterfaces": [
        {
          "Attachment": {
            "AttachTime": "2022-07-01T14:31:49+00:00",
            "AttachmentId": "eni-attach-09caf3c201ee6c473",
            "DeleteOnTermination": true,
            "DeviceIndex": 0,
            "Status": "attaching",
            "NetworkCardIndex": 0
          },
          "Description": "",
          "Groups": [
            {
              "GroupName": "ronin-ssh",
              "GroupId": "sg-60cbbd04"
            },
            {
              "GroupName": "INSPECTOR-SG",
              "GroupId": "sg-0ea6d866d0000000"
            }
          ],
          "Ipv6Addresses": [],
          "MacAddress": "02:83:e0:a5:5e:a2",
          "NetworkInterfaceId": "eni-99999999999",
          "OwnerId": "814453012568",
          "PrivateDnsName":
"ip-10-0-5-202.ap-southeast-2.compute.internal",
          "PrivateIpAddress": "10.0.5.202",
          "PrivateIpAddresses": [
            {
              "Primary": true,
              "PrivateDnsName":
"ip-10-0-5-202.ap-southeast-2.compute.internal",
              "PrivateIpAddress": "10.0.5.202"
            }
          ],
          "SourceDestCheck": true,
          "Status": "in-use",
          "SubnetId": "subnet-99999999999",
          "VpcId": "vpc-19c8e87c",
          "InterfaceType": "interface"
        }
      ],
      "RootDeviceName": "/dev/sda1",
      "RootDeviceType": "ebs",
      "SecurityGroups": [
        {
          "GroupName": "ronin-ssh",
          "GroupId": "sg-60cbbd04"
        },
        {
          "GroupName": "INSPECTOR-SG",
          "GroupId": "sg-0ea6d866d6a00b993"
        }
      ],
      "SourceDestCheck": true,
      "StateReason": {
        "Code": "pending",
        "Message": "pending"
      },
      "VirtualizationType": "hvm",
      "CpuOptions": {
        "CoreCount": 2,
        "ThreadsPerCore": 2
      },
      "CapacityReservationSpecification": {
        "CapacityReservationPreference": "open"
      },
      "MetadataOptions": {
        "State": "pending",
        "HttpTokens": "optional",
        "HttpPutResponseHopLimit": 1,
        "HttpEndpoint": "enabled",
        "HttpProtocolIpv6": "disabled"
      },
      "EnclaveOptions": {
        "Enabled": false
      }
    },
    "ebsConfig": [
      {
        "DeviceName": "/dev/sda1",
        "Ebs": {
          "DeleteOnTermination": true,
          "Encrypted": true,
          "VolumeSize": 10,
          "VolumeType": "gp2",
          "SnapshotId": "snap-08f2ffffffffff03a"
        }
      },
      {
        "DeviceName": "/dev/sdb",
        "Ebs": {
          "DeleteOnTermination": true,
          "Encrypted": true,
          "VolumeSize": "10",
          "VolumeType": "gp2"
        }
      }
    ]
  },
  "user_id": "batman+aa@ronin.cloud",
  "session_log": {
    "csrfp_ronin_token": [
      "24752ee9f8ff9189xxxxxxxxxxxxxxxx",
      "12d6b11d2ff61e2xxxxxxxxxxxxxxxxx"
    ],
    "CREATED": 1656685838,
    "auth": {
      "ChallengeParameters": [],
      "AuthenticationResult": {
        "AccessToken": "eyJraWQiOiXXXXXX",
        "ExpiresIn": 3600,
        "TokenType": "Bearer",
        "IdToken": "eyJraWQXXXXX",
        "RefreshToken": "eyJjdHkiXXXXXX"
      },
      "@metadata": {
        "statusCode": 200,
        "effectiveUri":
"https://cognito-idp.ap-southeast-2.amazonaws.com",
        "headers": {
          "date": "Fri, 01 Jul 2022 14:31:46 GMT",
          "content-type": "application/x-amz-json-1.1",
          "content-length": "2155",
          "connection": "keep-alive",
          "x-amzn-requestid":
"3764e3ba-7fe3-40cb-8f25-8eaeff2fe8e0"
        },
        "transferStats": {
          "http": [
            []
          ]
        }
      }
    },
    "user": {
      "Username": "batman+aa@ronin.cloud",
      "UserAttributes": [
        {
          "Name": "sub",
          "Value": "5dbee31f-eac5-483e-a1fa-8d4319e17368"
        },
        {
          "Name": "email_verified",
          "Value": "true"
        },
        {
          "Name": "email",
          "Value": "batman+aa@ronin.cloud"
        }
      ],
      "UserCreateDate": {
        "date": "2022-03-24 02:28:20.232000",
        "timezone_type": 3,
        "timezone": "UTC"
      },
      "UserLastModifiedDate": {
        "date": "2022-03-24 02:29:17.194000",
        "timezone_type": 3,
        "timezone": "UTC"
      },
      "Enabled": true,
      "UserStatus": "CONFIRMED",
      "@metadata": {
        "statusCode": 200,
        "effectiveUri":
"https://cognito-idp.ap-southeast-2.amazonaws.com",
        "headers": {
          "date": "Fri, 01 Jul 2022 14:30:39 GMT",
          "content-type": "application/x-amz-json-1.1",
          "content-length": "321",
          "connection": "keep-alive",
          "x-amzn-requestid":
"38c15d50-bc89-4925-b476-1b960fda37cb"
        },
        "transferStats": {
          "http": [
            []
          ]
        }
      },
      "sub": "5dbee31f-eac5-483e-a1fa-8d4319e17368",
      "email_verified": "true",
      "status": "success",
      "groups": [
        "ronin_admin",
        "INSPECTOR_admin"
      ]
    },
    "status": "success",
    "project": {
      "row_id": "1874",
      "name": "Ghost Inspector",
      "summary": "Project for automated testing of permissions and
other actions not covered by the PHANTOM project.",
      "tags": "automated,permissions,phantom,ghost,Inspector",
      "start_date": "13-12-2021",
      "end_date": "31-12-2022",
      "budget": "1000",
      "daily_limit": "",
      "over_notify": null,
      "over_limit": "0",
      "invoice_email": "\r\n
batman@ronin.cloud",
      "billing_code": "PHANTOM-123",
      "purchase_order": "INSPECTOR-123",
      "ts_created": "2021-12-13 03:24:14.257362+00",
      "ts_updated": null,
      "RPID": "INSPECTOR",
      "status": "",
      "custom_tags": null,
      "avatar":
"https://s3-ap-southeast-2.amazonaws.com/s3.ronin.cloud/INSPECTOR/
project_img_250x250.png",
      "aws": {
        "subnet": {
          "row_id": "39",
          "RPID": "INSPECTOR",
          "CIDR": "10.0.5.192/27",
          "ts_created": "2021-12-13 03:24:23.610719+00",
          "ts_updated": "2021-12-13 03:24:23.610719+00",
          "status": "CURRENT",
          "subnet_id": "subnet-99999999999"
        },
        "sg": "sg-0ea6d866d6a00b993"
      }
    }
  },
  "remote_address": "52.62.56.25",
  "server_log": {
    "HTTPS": "on",
    "SSL_TLS_SNI": "test.ronin.cloud",
    "HTTP_HOST": "test.ronin.cloud",
    "HTTP_CONNECTION": "keep-alive",
    "CONTENT_LENGTH": "254",
    "HTTP_SEC_CH_UA": "",
    "HTTP_SEC_CH_UA_MOBILE": "?0",
    "HTTP_USER_AGENT": "Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0 Safari/537.36
Ghost Inspector (62befde4c92ff234665745cb)",
    "CONTENT_TYPE": "application/x-www-form-urlencoded;
charset=UTF-8",
    "HTTP_ACCEPT": "*/*",
    "HTTP_X_REQUESTED_WITH": "XMLHttpRequest",
    "HTTP_SEC_CH_UA_PLATFORM": "",
    "HTTP_ORIGIN": "https://test.ronin.cloud",
    "HTTP_SEC_FETCH_SITE": "same-origin",
    "HTTP_SEC_FETCH_MODE": "cors",
    "HTTP_SEC_FETCH_DEST": "empty",
    "HTTP_REFERER": "https://test.ronin.cloud/instance.php",
    "HTTP_ACCEPT_ENCODING": "gzip, deflate, br",
    "HTTP_ACCEPT_LANGUAGE": "en-US",
    "HTTP_COOKIE":
"ronin_secure_session=gul7n0r6s3q9gc1iqpuofbng80;
csrfp_ronin_token=24752ee9f8ff9189943232b6788e05e8",
    "PATH":
"/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/sna
p/bin",
    "SERVER_SIGNATURE": "",
    "SERVER_SOFTWARE": "Apache",
    "SERVER_NAME": "test.ronin.cloud",
    "SERVER_ADDR": "10.0.2.17",
    "SERVER_PORT": "443",
    "REMOTE_ADDR": "52.62.56.25",
    "DOCUMENT_ROOT": "/var/www/html",
    "REQUEST_SCHEME": "https",
    "CONTEXT_PREFIX": "",
    "CONTEXT_DOCUMENT_ROOT": "/var/www/html",
    "SERVER_ADMIN": "admin@ronin.cloud",
    "SCRIPT_FILENAME":
"/var/www/html/ws/aws/ec2/create_machine.php",
    "REMOTE_PORT": "55793",
    "GATEWAY_INTERFACE": "CGI/1.1",
    "SERVER_PROTOCOL": "HTTP/1.1",
    "REQUEST_METHOD": "POST",
    "QUERY_STRING": "",
    "REQUEST_URI": "/ws/aws/ec2/create_machine.php",
    "SCRIPT_NAME": "/ws/aws/ec2/create_machine.php",
    "PHP_SELF": "/ws/aws/ec2/create_machine.php",
    "REQUEST_TIME_FLOAT": 1656685906.432,
    "REQUEST_TIME": 1656685906
  }
}
```