

Overview:

If working on an outside network, an unknown IP attacker can gain access to your virtual server. If this attacker has privileged access to the server, the attacker could use API calls to terminate an instance, or even import an image to the instance with planted malware.



Discovery:

There are 2 ways to discover an attack:

1. By using the API to checking logging information
2. Viewing the status of instances

The status checks can fail for multiple reasons

- Exhausted Memory
- Corrupted File Systems
- Incompatible Kernel

Any of these can fail for reasons as simple as the configuration was done incorrectly. By keeping a constant eye on the status of the instances can help to reduce the number of reasons why they may have failed. If a status fails unexpectedly, it can be thought that someone has uploaded an image with planted malware.

To View a Status Check

1. Login to Amazon EC2 console
2. Go to Instances from the Navigation Pane
3. Check the status lists on instances page
4. To view more detail about the status of a specific instance, choose Status Checks Tab

The screenshot shows the AWS Management Console interface for an EC2 instance. At the top, there are tabs for 'Description', 'Status Checks' (which is selected), 'Monitoring', and 'Tags'. Below the tabs, a message states: 'Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks.' There is a button labeled 'Create Status Check Alarm'. The main content area is divided into two columns. The left column is titled 'System Status Checks' with an information icon. It contains the text: 'These checks monitor the AWS systems required to use this instance and ensure they are functioning properly.' and a green status message: 'System reachability check passed'. The right column is titled 'Instance Status Checks' with an information icon. It contains the text: 'These checks monitor your software and network configuration for this instance.' and a red status message: 'Instance reachability check failed at October 7, 2013 11:52:11 AM UTC+2 (16 minutes ago)'. Below this message is a link: 'Learn more about this issue'. At the bottom, there is a section titled 'Additional Resources' with a link to 'Submit feedback' and a note about customer support.

For more information about status checks:

<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring-system-instance-status-check.html>

For more information about Access to EC2 Resources


<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/UsingIAM.html>

Remediation:

To remediate remote ssh/rdp access, it is important that privacy setting are put in place and the security checks are enforced. Another important thing would be to go back to the development stage and lock down ports other than Port 22 (SSH) and Port 3389 (RDP).

Delete the ssh port to keep your instance more secure

1 Security Group selected


 **Security Group: sg-71786b1d**

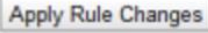
Details **Inbound*** **Outbound***

Create a new rule: Custom TCP rule

Port range:
(e.g., 80 or 49152-65535)

Source:
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

 Add Rule

 Apply Rule Changes

TCP (6)		
Port (Service)	Source	Action
80 (HTTP)	0.0.0.0/0	Delete
22 (SSH)	206.209.15.0/24	Delete
443 (HTTPS)	0.0.0.0/0	Delete

Prevention:

The best way to prevent an attack to the instance is by checking for intrusion during development

1. Lock down ports to prevent unauthorized access -- Port 22 (SSH) and 3389 (RDP) should only allow access on your private network
2. Also, restrict public internet access
3. Ditch passwords and require administrators to use SSH keys