

Sprint 8

CloudTrail & Audit Logs

CloudTrail access status: access

Purpose: Audit log for user log-in attempts & password changes

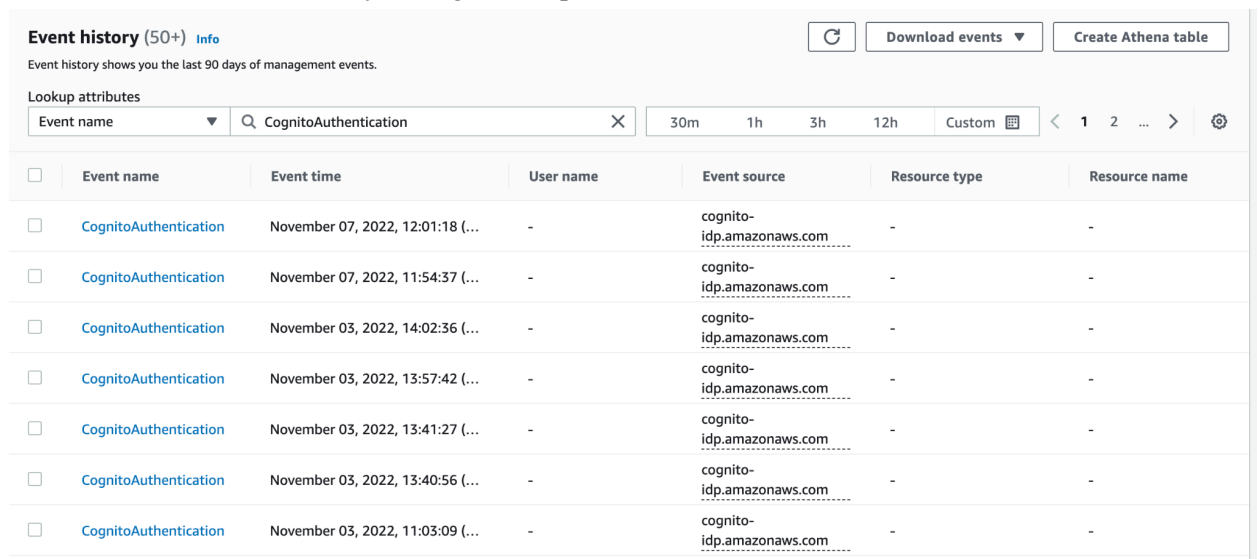
https://docs.amazonaws.cn/en_us/cognito/latest/developerguide/amazon-cognito-info-in-cloudtrail.html

Configuration Info:

- Encryption is enabled to encrypt log files containing user information
- S3 Bucket: aws-cloudtrail-logs-274815321855-025e3960
- Trail: Team21-CognitoTrail
- AWS KMS Alias: Team21-cognitokey

How to access the logs:

- CognitoAuthentication -> login attempts
 - Cloudtrail event history for login attempts:



The screenshot shows the AWS CloudTrail 'Event history' page. At the top, it says 'Event history (50+) Info' and 'Event history shows you the last 90 days of management events.' There are buttons for 'Download events' and 'Create Athena table'. Below this is a search bar with 'CognitoAuthentication' entered. The table below has columns: Event name, Event time, User name, Event source, Resource type, and Resource name. It lists several 'CognitoAuthentication' events from November 03, 2022, and November 07, 2022, all with a user name of '-' and event source of 'cognito-idp.amazonaws.com'.

<input type="checkbox"/>	Event name	Event time	User name	Event source	Resource type	Resource name
<input type="checkbox"/>	CognitoAuthentication	November 07, 2022, 12:01:18 (...)	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	CognitoAuthentication	November 07, 2022, 11:54:37 (...)	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	CognitoAuthentication	November 03, 2022, 14:02:36 (...)	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	CognitoAuthentication	November 03, 2022, 13:57:42 (...)	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	CognitoAuthentication	November 03, 2022, 13:41:27 (...)	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	CognitoAuthentication	November 03, 2022, 13:40:56 (...)	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	CognitoAuthentication	November 03, 2022, 11:03:09 (...)	-	cognito-idp.amazonaws.com	-	-

- Can download as CSV or JSON
- [ConfirmForgotPassword](#), forgotPassword, confirmgetpassword_post -> Cognito Password changes
 - New password: \$amTest123

Event history (8) Info <div> <div>🔄</div> <div>Download events ▾</div> <div>Create Athena table</div> </div>						
Event history shows you the last 90 days of management events.						
Lookup attributes <div> <div>Event name ▾</div> <div> <input type="text" value="ConfirmForgotPassword_POST"/> <div>✕</div> </div> <div> <div>30m</div> <div>1h</div> <div>3h</div> <div>12h</div> <div>Custom <div>📅</div></div> </div> <div> <div><</div> <div>1</div> <div>></div> <div>⚙️</div> </div> </div>						
<input type="checkbox"/>	Event name	Event time	User name	Event source	Resource type	Resource name
<input type="checkbox"/>	ConfirmForgotPassw...	November 07, 2022, 12:08:07 (...)	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	ConfirmForgotPassw...	October 24, 2022, 08:16:53 (UT...	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	ConfirmForgotPassw...	October 20, 2022, 10:41:53 (UT...	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	ConfirmForgotPassw...	October 20, 2022, 09:20:01 (UT...	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	ConfirmForgotPassw...	October 20, 2022, 09:19:41 (UT...	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	ConfirmForgotPassw...	October 20, 2022, 09:16:09 (UT...	-	cognito-idp.amazonaws.com	-	-
<input type="checkbox"/>	ConfirmForgotPassw...	October 20, 2022, 09:14:20 (UT...	-	cognito-idp.amazonaws.com	-	-

- Management events for API activity
 - https://docs.amazonaws.cn/en_us/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.html

Links:

<https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pool-settings-adaptive-authentication.html>

<https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-settings-viewing-advanced-security-metrics.html>

Load Balancer & WAF

- **ALB Info:**
 - Target Group: Team21-TargetGroup
 - Http protocol - port 80
 - Port that apache listens to

```
ubuntu@ip-10-0-0-9:/etc/apache2$ cat ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
ubuntu@ip-10-0-0-9:/etc/apache2$
```

- LB sends traffic to that
- Team21 VPC

Target Group:

EC2 > Target groups

Target groups (1) [Info](#) [Actions](#) [Create target group](#)

<input type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
<input type="checkbox"/>	Team21-TargetGroup	arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/team21-targetgroup/vpc-01234567	80	HTTP	Instance	None associated	vpc-01234567

Load Balancer:

Summary
Review and confirm your configurations. [Estimate cost](#)

Basic configuration Edit Team21-ALB <ul style="list-style-type: none">Internet-facingIPv4	Security groups Edit <ul style="list-style-type: none">Team21-SecurityGroup sg-089ea7302f44c5db2	Network mapping Edit VPC vpc-05fe4143ac3d5ca06 Team21-vpc <ul style="list-style-type: none">us-east-1b subnet-028634470d41441ce Team21-subnet-public2-us-east-1b	Listeners and routing Edit <ul style="list-style-type: none">HTTP:80 defaults to Team21-TargetGroup
Add-on services Edit None	Tags Edit None		
Attributes <div>i Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.</div>			

WAF ACL:

- Team21WAF-alb
- SQL Database managed rule

AWS WAF > Web ACLs > Team21-WAFalb

Team21-WAFalb

[Download web ACL as JSON](#)

[Overview](#) | **[Rules](#)** | [Bot Control](#) | [Associated AWS resources](#) | [Custom response bodies](#) | [Logging and metrics](#) | [CloudWatch Log Insights](#) [New](#)

[i](#) **New AWS managed rule group available: Account takeover prevention**
Protect your sign-in page against brute force and credential stuffing attacks. Account takeover prevention detects and mitigates against login attempts by malicious actors using stolen credentials. [Add to web ACL](#) [X](#)

Rules (1) [Edit](#) [Delete](#) [Add rules](#)

<input type="checkbox"/>	Name	Action	Priority	Custom response
<input type="checkbox"/>	AWS-AWSManagedRulesSQLiRuleSet	Use rule actions	0	-

Web ACL rule capacity units used
The total capacity units used by the web ACL can't exceed 1500.
[200/1500 WCUs](#)

Ideas:

- SNS “notification delivery” for other audit logs to also configure messages?

Notes:

- Next Sprint:
 - Fix the scalability issue
 - Grey out buttons if profile has not been completed
 - Welcome username will become first and last name
 - Make it say “please complete your profile” if they have not entered a name
 - View as a driver
 - Driver information, listing all sponsors
 - Sponsor information, listing all drivers