VECTRA

DATA SHEET

Vectra SaaS AWS CloudTrail metadata attributes and descriptions

This document describes the attributes in the AWS CloudTrail metadata data source supported by the Vectra AI Cloud Platform

AWS CloudTrail metadata	
Field	**Description**
timestamp	Time when the event happened
event_version	The version of the CloudTrail log event format
user_identity.type	The type of the identity. Examples: Root, IAMUser, AssumedRole, Role, FederatedUser, etc
user_identity.principal_id	A unique identifier for the entity that made the call
user_identity.arn	The Amazon Resource Name (ARN) of the principal that made the call. The last section of the arn contains the user or role that made the call
user_identity.account_id	The account that owns the entity that granted permissions for the request
user_identity.access_key_id	The access key ID that was used to sign the request
user_identity.session_context.session_issuer.type	If the request was made with temporary security credentials, sessionContext provides information about the session that was created for those credentials. In this case, the identity type
user_identity.session_context.session_issuer.principal_id	If the request was made with temporary security credentials, sessionContext provides information about the session that was created for those credentials; in this case, a unique identifier for the entity that made the call
user_identity.session_context.session_issuer.arn	If the request was made with temporary security credentials, sessionContext provides information about the session that was created for those credentials; in this case, The Amazon Resource Name (ARN) of the principal that made the call. The last section of the arn contains the user or role that made the call
user_identity.session_context.session_issuer.account_id	If the request was made with temporary security credentials, sessionContext provides information about the session that was created for those credentials; in this case, the account that owns the entity that granted permissions for the request

AWS CloudTrail metadata	
Field	**Description**
user_identity.session_context.session_issuer.user_name	If the request was made with temporary security credentials, sessionContext provides information about the session that was created for those credentials; in this case, the friendly name of the identity that made the call
user_identity.session_context.attributes.mfa_authenticated	If the request was made with temporary security credentials, sessionContext provides information about the session that was created for those credentials; in this case, if the root user or IAM user whose credentials were used for the request also was authenticated with an MFA device
user_identity.session_context.attributes.creation_date	If the request was made with temporary security credentials, sessionContext provides information about the session that was created for those credentials; in this case, the date and time when the temporary security credentials were issued
user_identity.session_context.ec2_role_delivery	The version of the IMDS API used to retrieve credentials for an EC2. This is only applicable for ec2 instances. It can be null, 1, or 2
user_identity.session_context.source_identity	Identifies the original user identity making the request, whether that user's identity is an IAM user, an IAM role, a user authenticated through SAML-based federation, or a user authenticated through OpenID Connect (OIDC)-compliant web identity federation.
user_identity.user_name	The friendly name of the identity that made the call
user_identity.invoked_by	The name of the AWS service that made the request, such as Amazon EC2 Auto Scaling or AWS Elastic Beanstalk
event_time	The date and time the request was made, in coordinated universal time (UTC)
event_source	The service that the request was made to. This name is typically a short form of the service name without spaces plus .amazonaws.com
event_name	The requested action, which is one of the actions in the API for that service

AWS CloudTrail metadata	
Field	**Description**
aws_region	The AWS region that the request was made to, such as us-east-2
source_ip_address	The IP address that the request was made from. For actions that originate from the service console, the address reported is for the underlying customer resource, not the console web server. When a service is accessed on behalf of a console user ip address of "AWS_INTERNAL" is used
source_ip_address	The IP address that the request was made from. For actions that originate from the service console, the address reported is for the underlying customer resource, not the console web server. When a service is accessed on behalf of a console user ip address of "AWS_INTERNAL" is used
user_agent	The agent through which the request was made, such as the AWS Management Console, an AWS service, the AWS SDKs or the AWS CLI
request_parameters	The parameters, if any, that were sent with the request
request_source_identity.value	Identity responsible for a given action. This field can be populated when a third-party identity provider (IdP) is used
assume_role_role_arn	The role ARN request parameter for an AssumeRole event
response_elements	The response element for actions that make changes (create, update, or delete actions)
request_id	The value that identifies the request. The service being called generates this value
event_id	GUID generated by CloudTrail to uniquely identify each event
resources.0.arn	ARN of resource(s) accessed in the event
resources.0.account_id	Account ID of the resource owner
resources.0.type	Resource type identifier in the format: AWS::aws-service-name::data-type-name
event_type	Identifies the type of event that generated the event record
recipient_account_id	Represents the account ID that received this event
shared_event_id	GUID generated by CloudTrail to uniquely identify CloudTrail events from the same AWS action that is sent to different AWS accounts

AWS CloudTrail metadata	
Field	**Description**
error_code	The AWS service error code, if the request returns an error
error_message	If the request returns an error, the description of the error
api_version	Identifies the API version associated with the AwsApiCalleventType value
read_only	Identifies whether this operation is a read-only operation
additional_event_data	Additional data about the event that was not part of the request or response
vpc_endpoint_id	Identifies the VPC endpoint in which requests were made from a VPC to another AWS service, such as Amazon S3
event_category	Shows the event category that is used in LookupEvents calls
session_credential_from_console	Shows whether or not an event originated from an AWS Management Console session
management_event	A Boolean value that identifies whether the event is a management event
service_event_details	Identifies the service event, including what triggered the event and the result
vectra.entity.resolved_identity.identity_type	Identity type of the original user identity before any other roles were assumed
vectra.entity.resolved_identity.canonical_name	Name of the Kingpin Attributed entity which performed this action, regardless of roles assumed
vectra.entity.resolved_identity.account_id	IAM user account_id before any other roles were assumed
vectra.entity.resolved_identity.principal_id	Principal ID of the IAM user before any other roles were assumed
vectra.entity.resolved_identity.user_name	Username associated to the IAM user, before any other roles were assumed
vectra.entity.resolved_identity.arn	IAM user ARN before any other roles were assumed
vectra.entity.resolved_identity.invoked_by	Resolved identity of the AWS Service (null if it's not a service)
vectra.entity.resolved_identity.aws_region	The AWS region where the original action was taken by the resolved identity

AWS CloudTrail metadata	
Field	**Description**
vectra.entity.role_ chain.0.arn	The ARN of the first role the user automatically assumed, before any other roles were assumed
vectra.entity.role_ chain.0.principal_id	The principal ID of the role session, which includes the principal ID of the role and the name of the role session separated by a colon
vectra.entity.role_ chain.0.creation_date	The creation date of the role session. Basically, the date and time when the role was assumed
vectra.entity.role_ chain.0.role_session_name	The role session's session name
vectra.entity.role_ chain.0.aws_access_key	The role session's access key id

For more information about Vectra metadata attributes, please contact a service representative or email us at info@vectra.ai.

Email info@vectra.ai vectra.ai