cloud events

ONTAP 9.11.1 EMS reference

NetApp
December 15, 2022

Table of Contents

cloud events

cloud.aws events

cloud.aws.iamCredsExpired

Severity

ERROR

Description

This message occurs when the IAM Role thread acquires Amazon Web Services (AWS) Identity and Access Management (IAM) role-based credentials that have already expired. The credentials are acquired from the AWS metadata server using the IAM role, and are used in signing API requests to AWS S3.

Corrective Action

Log in to the AWS EC2 Management Console, click on the 'Instances' page, and then find and check the health of the instance pertaining to this ONTAP Cloud deployment. Also verify that the AWS IAM role associated with the instance exists and grants proper privileges to the instance.

Syslog Message

ONTAP acquired AWS credentials associated with the AWS IAM role named '%s' on the AWS metadata server that have already expired. Node %s.

Parameters

iamRole (STRING): Name of the IAM role associated with this ONTAP Cloud® instance.
nodeUuid (STRING): UUID of the node.

cloud.aws.iamCredsInvalid

Severity

ERROR

Description

This message occurs when the system acquires Amazon Web Services (AWS) Identity and Access Management (IAM) role-based credentials that are not valid.

Corrective Action

In the AWS EC2 Management Console, find and check the health of the instance pertaining to this ONTAP Cloud deployment. Also, verify that the AWS IAM role associated with the instance exists and grants proper privileges to the instance.

Syslog Message

AWS credentials that were acquired by ONTAP are not valid. AWS IAM role: %s. Node: %s.

Parameters

iamRole (STRING): Name of the IAM role associated with this ONTAP Cloud instance.
nodeUuid (STRING): UUID of the node.

cloud.aws.iamCredsNotFound

Severity

ERROR

Description

This message occurs when the cloud credentials thread cannot acquire Amazon Web Services (AWS) Identity and Access Management (IAM) role-based credentials from the AWS metadata server. The credentials are used in signing API requests to AWS S3.

Corrective Action

Log in to the AWS EC2 Management Console, click on the 'Instances' page, and then find and check the health of the instance pertaining to this Cloud Volumes ONTAP® deployment. Also verify that the AWS IAM role associated with the instance exists and grants proper privileges to the instance.

Syslog Message

ONTAP cannot acquire credentials associated with the AWS IAM role or GCP Service Account named '%s' on the metadata server. Node %s.

Parameters

iamRole (STRING): Name of the AWS IAM role associated associated with this Cloud Volumes ONTAP® instance.
nodeUuid (STRING): UUID of the node.

cloud.aws.iamNotInitialized

Severity

NOTICE

Description

This message occurs when a module attempts to access Amazon Web Services (AWS) Identity and Access Management (IAM) role-based credentials from the cloud credentials thread before the cloud thread is finished initializing.

Corrective Action

Wait for the cloud credential thread, and by extension the system, to complete initialization.

Syslog Message

A module attempted to access credential information before the cloud credential thread initialized on node %s.

Parameters

nodeUuid (STRING): UUID of the node.

cloud.aws.iamRoleInvalid

Severity

ERROR

Description

This message occurs when the system acquires an Amazon Web Services (AWS) Identity and Access Management (IAM) role on the AWS metadata server that is not valid.

Corrective Action

In the AWS EC2 Management Console, find and check the health of the instance pertaining to this ONTAP Cloud deployment. Also, verify that the AWS IAM role associated with the instance exists and grants proper privileges to the instance.

Syslog Message

IAM role "%s" on the AWS metadata server is not valid for this ONTAP instance (node %s).

Parameters

iamRole (STRING): Name of the IAM role associated with this ONTAP Cloud instance.
nodeUuid (STRING): UUID of the node.

cloud.aws.iamRoleNotFound

Severity

ERROR

Description

This message occurs when the IAM Role thread cannot find an Amazon Web Services (AWS) Identity and Access Management (IAM) role on the AWS metadata server. The IAM role is needed to obtain role-based credentials used in signing API requests to AWS S3.

Corrective Action

Log in to the AWS EC2 Management Console, click on the 'Instances' page, and then find and check the health of the instance pertaining to this ONTAP Cloud® deployment. Also verify that the AWS IAM role associated with the instance exists.

Syslog Message

ONTAP node %s cannot find an IAM role on the AWS metadata server.

Parameters

nodeUuid (STRING): UUID of the node.

cloud.aws.metadataConnFail

Severity

ERROR

Description

This message occurs when the IAM Role thread cannot establish a communication link with the Amazon Web Services (AWS) metadata server. Communication must be established to acquire the necessary AWS Identity and Access Management (IAM) role-based credentials used in signing API requests to AWS S3.

Corrective Action

Log in to the AWS EC2 Engine Management Console, click on the 'Instances' page, and then find and check the health of the instance pertaining to this Cloud Volumes ONTAP® deployment.

Syslog Message

ONTAP cannot communicate with the AWS metadata server needed to acquire IAM role-based or Service Account based credentials for access to AWS S3 Storage. Error returned: %s Node: %s

Parameters

error (STRING): Error code and string, if applicable.
nodeUuid (STRING): UUID of the node.

cloud.azurecredsinvalid events

cloud.azureCredsInvalid

Severity

ERROR

Description

This message occurs when the system acquires Azure Managed Service Identity (MSI) credentials that are not valid.

Corrective Action

In the Azure Portal, find and check the health of the instance pertaining to this Cloud Volumes ONTAP® deployment. Also, verify that the MSI associated with the instance is enabled and grants proper privileges to the instance.

Syslog Message

Azure MSI credentials that were acquired by ONTAP are not valid. Node UUID: %s.

Parameters

nodeUuid (STRING): UUID of the node.

cloud.creds events

cloud.creds.metadataConnFail

Severity

ERROR

Description

This message occurs when the system cannot establish a communication link with the cloud provider’s metadata server, in order to acquire the necessary temporary credentials used in signing API requests to the cloud object store server.

Corrective Action

Log in to the cloud provider’s management console to examine the current set of running instances. Find the instance pertaining to this deployment of Cloud Volumes ONTAP® deployment, and then check its health from the console.

Syslog Message

ONTAP cannot communicate with the cloud provider’s metadata server needed to acquire the temporary credentials used to access an object store server. Command: %s Error returned: %s Node: %s

Parameters

command (STRING): Command used to contact the metadata server.
error (STRING): Error text received as response to the metadata server command.

nodeUuid (STRING): UUID of the node.

cloud.creds.notFound

Severity

ERROR

Description

This message occurs when the system cannot acquire the temporary credentials from the cloud provider's metadata server that are necessary for signing API requests to the object storage server.

Corrective Action

Log in to the management console of the cloud provider to examine the current set of running instances. Find and check the health of the instance pertaining to this Cloud Volumes ONTAP deployment. Also verify that the role associated with the instance exists and grants the proper privileges.

Syslog Message

ONTAP cannot acquire credentials associated with the instance named '%s' on the metadata server. Node %s.

Parameters

role (STRING): Name of the AWS IAM role or GCP Service Account or Azure Managed Service Identity associated with this Cloud Volumes ONTAP® instance.
nodeUuid (STRING): UUID of the node.

cloud.creds.notInitialized

Severity

NOTICE

Description

This message occurs when the system attempts to access credentials before initialization is complete.

Corrective Action

(None).

Syslog Message

Module on node %s attempted to access credential information before initialization was complete

Parameters

nodeUuid (STRING): UUID of the node.

cloud.gcpcredsinvalid events

cloud.gcpCredsInvalid

Severity

ERROR

Description

This message occurs when the system acquires Google Cloud Platform (GCP) Service Account based credentials that are not valid.

Corrective Action

In the Google Cloud Console, find and check the health of the instance pertaining to this Cloud Volumes ONTAP® deployment. Also, verify that the Service Account associated with the instance exists and grants proper privileges to the instance.

Syslog Message

GCP credentials that were acquired by ONTAP are not valid. Node: %s.

Parameters

nodeUuid (STRING): UUID of the node.

Copyright information

Trademark information