nblade events

ONTAP 9.11.1 EMS reference

NetApp
December 15, 2022

Table of Contents

nblade events

nblade.callbacktimedout events

Nblade.CallbackTimedOut

Severity

ERROR

Description

This message occurs when the Nblade is unable to successfully complete a PORTMAP/SM call to the client within 1 seconds. The PORTMAP/SM calls are done as part of the per-aggregate lock reclaim process after a Dblade reboot. If a large number of such calls fail for a particular aggregate, then it delays the completion of the lock reclaim process for that aggregate. That delay prevents the aggregate from granting new locks to NFS clients.

Corrective Action

Check if the RPC program number displayed above with the correct program version is running on the client and if not start it. You can use "rpcinfo -p" on the client to check that. It is also possible that the client is unreachable due to firewall/network connectivity issues.

Syslog Message

SM NOTIFY: Vserver %d, Vif %d: %s program (Program number:%d Program version:%d) on client %s is not responding.

Parameters

virtualServer (INT): Identifier for the Vserver associated with this operation.
lifId (INT): Identifier for the logical interface associated with this operation.
program (STRING): Client program not responding.
programNum (INT): RPC Program Number.
programVersion (INT): RPC Program Version.
remoteIpAddress (STRING): IP address of the client machine.

nblade.cifs events

Nblade.cifs.budgetAllocFailure

Severity

ERROR

Description

This message occurs when there is a budget allocation failure for a CIFS subsystem because other CIFS subsystems are consuming too much memory. The three displayed CIFS subsystem have consumed most of the memory.

Corrective Action

Consider distributing the CIFS load by moving data LIFs, adding data LIFs, and redirecting workloads, or by shutting down nonessential workloads to alleviate the memory pressure. If the problem persists after addressing issues on the network or the client, contact NetApp technical support.

Syslog Message

Memory Allocation failed for %s. The CIFS subsystem on this node has exceeded its allotment of %llu bytes of node memory. CIFS subsystems that have consumed the most memory are %s.

Parameters

budgetname (STRING): Name of the CIFS subsystem for which memory allocation failed.
TotalCifsBudget (LONGINT): Amount of memory available to the CIFS subsystem.
topConsumers (STRING): CIFS subsystem that have consumed the most memory, and the amount of memory consumed.

Nblade.cifs.logon.audit.fail

Severity

ERROR

Description

This message occurs when a CIFS logon fails when guaranteed audit is enabled and audit log generation fails due to no space remaining in either destination volumes or staging volumes.

Corrective Action

Use the command "event log show -messagename adt.service.block" to check for destination volume space unavailability. If the message entry exists, use the command "event log show -messagename adt.service.block -fields action" and follow the corrective action. If the message entry does not exist, then staging volumes are full and no corrective action is necessary. The audit process self-heals and normal auditing continues in 10 seconds after audit logging cleanup occurs.

Syslog Message

CIFS logon failed due to audit log generation failure for the vserver %u.

Parameters

vsId (INT): Id of the vserver, on which this event occurred.

nblade.cifsencsessaccessdenied events

Nblade.cifsEncSessAccessDenied

Severity

ERROR

Description

This message occurs when a client not capable of SMB encryption tries to establish a CIFS session that requires SMB encryption.

Corrective Action

Either ensure that the client is capable of SMB encryption or disable SMB encryption on the Vserver.

Syslog Message

Client (IP: %s, Vserver: %d) could not establish a CIFS session because SMB encryption is required.

Parameters

IpAddress (STRING): IP address of the client attempting to establish a CIFS session.
vserverId (INT): Identifier of the Vserver associated with this operation.

nblade.cifsencshraccessdenied events

Nblade.cifsEncShrAccessDenied

Severity

ERROR

Description

This message occurs when a client not capable of SMB encryption tries to connect to a CIFS share that requires SMB encryption.

Corrective Action

Either ensure that the client is capable of SMB encryption or disable SMB encryption on the CIFS share.

Syslog Message

Client (IP: %s, Vserver: %d) could not connect to CIFS share "%s" because SMB encryption is required.

Parameters

IpAddress (STRING): IP address of the client from which Share Connect requests are being attempted.
vserverId (INT): Identifier of the Vserver associated with this operation.
shareName (STRING): Name of the share to which the client is connecting.

nblade.cifsetcdactionfailed events

Nblade.cifsEtcdActionFailed

Severity

ERROR

Description

This message occurs when the DMAP container encounters an error processing an etcd request, such as a connection failure.

Corrective Action

Check the network connectivity of the etcd server to the ONNIX pod, and correct any networking faults. Scan the DMAP and etcd logs for additional information.

Syslog Message

Received an etcd failure event, Message is %s.

Parameters

pMessage (STRING): Description of the SMB configuration update failure.

nblade.cifsetcdmaxtxnlimit events

Nblade.cifsEtcdMaxTxnLimit

Severity

ERROR

Description

This message occurs when the number of Access Control Entries (ACE) present in an MSRPC request for updating share permissions exceeds the supported maximum etcd limit of 1,022 entries.

Corrective Action

Retry the operation with less than the maximum supported number of ACEs in the MSRPC request.

Syslog Message

Received an etcd failure event. Message is %s.

Parameters

pMessage (STRING): Description of the error.

nblade.cifslongrunpattmatch events

Nblade.CifsLongRunPattMatch

Severity

ERROR

Description

This message occurs when a CIFS query directory command that includes wildcard characters exceeds the reporting time threshold for completion. Pattern-matching searches on strings including wildcard characters consume excessive CPU resources.

Corrective Action

Check the Windows client that is requesting searches containing wildcard characters. For assistance, contact NetApp technical support.

Syslog Message

Detected a long running CIFS pattern matching operation. SMB dialect: %s Allowed pattern matching threshold (ms): %llu Total pattern matching time taken(ms): %llu Client IP address: %s Target Vserver name: %s Target Vserver ID: %d Wildcard Pattern: %s Share name: %s Directory Path: %s

Parameters

dialect (STRING): Negotiated SMB dialect.
allowedThresholdInMs (LONGINT): Pattern-matching threshold value.
totalTimeTakenInMs (LONGINT): Total time taken for pattern matching.
clientIpAddress (STRING): IP address of the client machine.
vservername (STRING): Identifier for the Vserver name associated with this operation.
vserverId (INT): Identifier for the Vserver associated with this operation.
pattern (STRING): Wildcard pattern sent.
shareName (STRING): Target share name.
dirPath (STRING): Target directory path.

nblade.cifsmanyauths events

Nblade.cifsManyAuths

Severity

ERROR

Description

This message occurs when many authentication negotiations occur simultaneously. There are 256 new session requests from this client that are not yet complete.

Corrective Action

Investigate why the client is creating 256 or more new connection requests. It might be necessary to contact the vendor of the client or of the application in order to determine why this is occuring.

Syslog Message

Many simultaneous new CIFS connections are occurring on Vserver ID %u from IP address %s object type is %s with UUID %s.

Parameters

vsId (INT): ID of the Vserver on which this event occurred.
remoteIpAddress (STRING): IP address of the client machine.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the Vserver.

nblade.cifsmaxopensamefile events

Nblade.cifsMaxOpenSameFile

Severity

ERROR

Description

This message occurs when the number of times a user tries to open a file over a TCP connection is exceeded. This request and any further requests to open the same file by the user are denied until some open instances of the file are closed. This typically indicates abnormal application behavior.

Corrective Action

Inspect the application running on the client using this TCP connection. The client might be operating incorrectly due to the application running on it. Rebooting the client might also be helpful. In some cases, clients are operating as expected but require a higher threshold, which you can set using the (privilege: advanced) "cifs option modify -max-opens-same-file-per-tree" command.

Syslog Message

Received too many open file requests for the same file by one user on a connection: clientIP:port %s:%d, file "%s" on share "%s", vserver: "%s". Object type is: %s with UUID: %s.

Parameters

IpAddress (STRING): IP address of the client from which open requests are denied.
port (INT): Port number of the client from which the connection has been established.
filePath (STRING): Path of the file that cannot be opened.

shareName (STRING): Name of the share that holds the file.
vserverName (STRING): Vserver associated with this operation.
object_type (STRING): Type of resource object.
object_uuid (STRING): UUID of the resource object.

nblade.cifsmaxopensamefilenotice events

Nblade.cifsMaxOpenSameFileNotice

Severity

NOTICE

Description

This message occurs when the number of open instances of a particular file under a CIFS tree nears the configuration limit. Upon reaching this limit, any further requests to open the same file by the user are denied until some open instances of the file are closed. This typically indicates abnormal application behavior.

Corrective Action

Inspect the application running on the client using this TCP connection. The client might be operating incorrectly due to the application running on it. Rebooting the client might also be helpful. In some cases, clients are operating as expected but require a higher threshold, which you can set by using the (privilege: advanced) "cifs option modify -max-opens-same-file-per-tree" command.

Syslog Message

Received %d open file requests, nearing the configured limit of %d, for the same file by one user on a connection: clientIP:port %s:%d, file: "%s" on share: "%s", vserver: "%s".

Parameters

currentCount (INT): Current count of the open instances on the file.
maxValue (INT): Maximum allowed open instances on a file.
IpAddress (STRING): IP address of the client requesting the file open.
port (INT): Port number of the client from which the connection has been established.
filePath (STRING): Path of the file being opened.
shareName (STRING): Name of the share that holds the file.
vserverName (STRING): Vserver associated with this operation.

nblade.cifsmaxsessperusrconn events

Nblade.cifsMaxSessPerUsrConn

Severity

ERROR

Description

This message occurs when the number of sessions allowed per user over a TCP connection is exceeded. This request and any further session establishment requests are denied until some sessions are released. This is typically caused by a faulty client or application.

Corrective Action

Inspect all applications running on the client, and terminate any that are not operating properly. Rebooting the client might also be helpful. In some cases, clients are operating as expected but require a higher threshold, which you can set using the (privilege: advanced) "cifs option modify -max-same-user-sessions -per-connection" command.

Syslog Message

Received too many session requests from the same user on one TCP connection: clientIP:port %s:%d, user "%s", vserver: "%s". Object type is: %s with UUID: %s.

Parameters

IpAddress (STRING): IP address of the client requesting a session.
port (INT): Port number of the client from which the TCP connection has been established.
userName (STRING): User that has exceeded session requests.
vserverName (STRING): Vserver associated with this operation.
object_type (STRING): Type of resource object.
object_uuid (STRING): UUID of the resource object.

nblade.cifsmaxsessperusrconnnotice events

Nblade.cifsMaxSessPerUsrConnNotice

Severity

NOTICE

Description

This message occurs when the number of sessions allowed per user over a TCP connection nears the configured limit. Upon reaching this limit, any further session establishment requests are denied until some sessions are released. This is typically caused by a faulty client or application.

Corrective Action

Inspect all applications running on the client, and terminate any that are not operating properly. Rebooting the client might also be helpful. In some cases, clients are operating as expected but require a higher threshold, which you can set by using the (privilege: advanced) "cifs option modify -max-same-user -sessions-per-connection" command.

Syslog Message

Received %d session requests, nearing the configured limit of %d, from the same user on one TCP connection: clientIP:port %s:%d, user: "%s", vserver: "%s".

Parameters

currentCount (INT): Current count of the sessions.
maxValue (INT): Maximum allowed sessions per user over a TCP connection.
IpAddress (STRING): IP address of the client requesting a session.
port (INT): Port number of the client from which the TCP connection has been established.
userName (STRING): User that is nearing the session requests limit.
vserverName (STRING): Vserver associated with this operation.

nblade.cifsmaxwatchespertree events

Nblade.cifsMaxWatchesPerTree

Severity

ERROR

Description

This message occurs when the total number of directory watch (Change Notify) requests exceed the per-tree limit. This request and any further directory watch requests are denied. This typically indicates abnormal client behavior.

Corrective Action

Inspect the application using the connection and also monitor the other applications on the client. The client might be operating incorrectly due to a faulty application running on it. Rebooting the client might also be helpful. In some cases, clients are operating as expected but require a higher threshold, which can be set using the (privilege: advanced) "cifs option modify -max-watches-set-per-tree" command.

Syslog Message

Received too many Change Notify requests on one tree: clientIP:port %s:%d, directory "%s" on share "%s", vserver: "%s".

Parameters

IpAddress (STRING): IP address of the client requesting Change Notify functionality.
port (INT): Port number of the client from which the TCP connection has been established.
dirPath (STRING): Path of the directory on which Change Notify is requested.
shareName (STRING): Name of the share that holds the directory.
vserverName (STRING): Vserver associated with this operation.

nblade.cifsmaxwatchespertreenotice events

Nblade.cifsMaxWatchesPerTreeNotice

Severity

NOTICE

Description

This message occurs when the total number of directory watch (Change Notify) requests nears the configured limit. Upon reaching this limit, any further directory watch requests are denied. This typically indicates abnormal client behavior.

Corrective Action

Inspect the application using the connection, and also monitor the other applications on the client. The client might be operating incorrectly due to a faulty application running on it. Rebooting the client might also be helpful. In some cases, clients are operating as expected but require a higher threshold, which can be set by using the (privilege: advanced) "cifs option modify -max-watches-set-per-tree" command.

Syslog Message

Received %d Change Notify requests, nearing the configured limit of %d, on one tree: clientIP:port %s:%d, directory: "%s" on share: "%s", vserver: "%s".

Parameters

currentCount (INT): Current count of the Change Notify on the tree.

maxValue (INT): Maximum allowed Change Notify on the tree.
IpAddress (STRING): IP address of the client requesting Change Notify functionality.
port (INT): Port number of the client from which the TCP connection has been established.
dirPath (STRING): Path of the directory on which Change Notify is requested.
shareName (STRING): Name of the share that holds the directory.
vserverName (STRING): Vserver associated with this operation.

nblade.cifsmemexceeded events

Nblade.cifsMemExceeded

Severity

ERROR

Description

This message occurs when the CIFS subsystem, which operates all the CIFS servers exposed through a given node, has requested more memory than it is allowed in this node. The subsystem is restricted to a percentage of total memory in the node, so the node itself need not be low on memory for this to occur. CIFS memory is not allocated in advance and so CIFS memory requests compete with other system processes. This message might not appear if a memory request from CIFS cannot be honored because the node is already low on memory. This might result in CIFS client operation failures.

Corrective Action

Compare the number of memory allocation failures with the previous occurence of this event to understand the load on the system. Further analyze the memory allocated to the CIFS subsystem on this node by viewing the nblade_cifs object instance for this node through the "statistics show" interface. Based on that data, consider distributing CIFS load by moving data LIFs, adding data LIFs, and redirecting workloads, or by shutting down non-essential workloads to alleviate the memory pressure.

Syslog Message

The CIFS subsystem on this node has exceeded its allotment of %llu bytes of node memory with currently %llu memory allocation failures since boot time. This might result in unexpected CIFS application failures.

Parameters

availableMemoryInBytes (LONGINT): Amount of memory available to the CIFS subsystem.
memAllocFailures (LONGINT): Number of memory allocation failures in the CIFS subsystem since boot time.

nblade.cifsnbnameconflict events

Nblade.cifsNbNameConflict

Severity

ERROR

Description

This message occurs when the NetBIOS Name Service receives a negative response from a remote machine for a name registration request. This is typically caused by a conflict in the NetBIOS name or an alias. As a result, clients might not be able to access data or connect to the right data-serving node in the cluster.

Corrective Action

1. If applicable, delete the duplicate NetBIOS alias by using the "vserver cifs delete -aliases alias -vserver vserver" command. Alternatively, rename a NetBIOS alias by deleting the duplicate name and adding an alias with a new name by using the "vserver cifs create -aliases alias -vserver vserver" command. 2. If there are no aliases configured and there is a conflict in the NetBIOS name, then rename the CIFS server by using the "vserver cifs delete -vserver vserver" and "vserver cifs create -cifs-server netbiosname" commands. Note that deleting a CIFS server can cause data to be inaccessible. 3. Remove or rename the NetBIOS name on the remote machine.

Syslog Message

The NetBIOS Name Service received a negative name registration response. The name %s is owned by a remote machine. The IP address being registered is %s. Object type is: %s with UUID: %s.

Parameters

nbName (STRING): NetBIOS name or alias being registered by the NetBIOS Name Service.
IpAddress (STRING): IP address being registered by the NetBIOS Name Service.
object_type (STRING): Type of resource object.
object_uuid (STRING): UUID of the resource object.

nblade.cifsnonaesnibytesproc events

Nblade.cifsNonAesNiBytesProc

Severity

ALERT

Description

This message occurs when a system with CPUs that do not support the AES-NI instruction set is performing SMB3 encryption or signing of a large amount of data. These cryptographic operations can degrade performance severely for both SMB and other system operations.

Corrective Action

Avoid encrypted or signed SMB3 traffic on systems that do not support the AES-NI instruction set.

Syslog Message

Excessive SMB3 cryptographic processing load (AES-NI instruction set is not supported).

Parameters

(None).

nblade.cifsnonunicoderequest events

Nblade.cifsNonUnicodeRequest

Severity

ERROR

Description

This message occurs when a client attempts to send a non-unicode request to a Vserver. The request is rejected.

Corrective Action

Check the client to verify that it supports unicode characters and negotiates unicode support with the Vserver.

Syslog Message

Vserver ID %u rejected non-unicode request from client IP: %s.

Parameters

vserverId (INT): Identifier for the Vserver that received the non-unicode request.
clientIp (STRING): IP address of the client sending the non-unicode request.

nblade.cifsnoprivshare events

Nblade.cifsNoPrivShare

Severity

EMERGENCY

Description

This message occurs when a client attempts to connect to a nonexistent ONTAP_ADMIN$ share.

Corrective Action

Ensure that the vscan is enabled for the mentioned Vserver ID. Enabling vscan on a Vserver causes the ONTAP_ADMIN$ share to be created for the Vserver automatically.

Syslog Message

Vserver ID: %d, user name: %s, client ip: %s, Object type is: %s with UUID: %s.

Parameters

vserverId (INT): Identifier for the Vserver associated with this operation.
userName (STRING): User name of the client attemping to access the nonexistent ONTAP_ADMIN$ share.
clientIp (STRING): IP address of the client attemping to access the nonexistent ONTAP_ADMIN$ share.
object_type (STRING): Type of resource object.
object_uuid (STRING): UUID of the resource object.

nblade.cifsoperationtimedout events

Nblade.CifsOperationTimedOut

Severity

ERROR

Description

This message occurs when a CIFS operation times out because it could not be processed completely within 40 seconds.

Corrective Action

Check the QoS policy configuration for the target volume. If there are no QoS policies set, check the load on the target volume and check IP connectivity over the cluster interfaces between the two nodes. For further assistance, contact NetApp technical support and indicate that you need assistance with a potential

internal cluster performance problem.

Syslog Message

Detected a timed out CIFS operation. SMB command for this operation: %s, Number of times this command was suspended: %llu, Number of times this command was restarted: %llu, Last CSM error during this operation: %s, Remote blade UUID: %s, Is QoS enabled: %s, Last nBlade error during this operation: %s, Client IP address: %s, Local IP address: %s, Target Vserver ID: %d, Target disk's DSID: %d, Target Vserver Name: %s

Parameters

commandName (STRING): CIFS command for this operation.
suspensionCnt (LONGINT): Number of times this command has been suspended.
cmdRestartCnt (LONGINT): Number of times this command has been restarted.
lastCsmError (STRING): Last CSM error.
remoteBladeID (STRING): Remote blade ID for this CSM session.
isQosEnabled (STRING): Whether QoS is enabled.
lastSpinNpError (STRING): Last internal network component(nBlade) error.
clientIpAddress (STRING): IP address of the client machine.
localIpAddress (STRING): IP address of the local interface serving the protocol operation.
vserverId (INT): Identifier for the Vserver associated with this operation.
dsId (INT): Data set ID (DSID) of the target volume.
vserverName (STRING): Vserver name associated with this operation.

nblade.cifssametreepersess events

Nblade.cifsSameTreePerSess

Severity

ERROR

Description

This message occurs when the number of connections to the same share allowed per session is exceeded. This request and any further requests to establish another connection to that share are denied until some connections to the share are released. This typically indicates abnormal client behavior.

Corrective Action

Inspect the application using the connection and also monitor the other applications on the client. The client might be operating incorrectly due to a faulty application running on it. Rebooting the client might also be helpful. In some cases, clients are operating as expected but require a higher threshold, which you can set using (privilege: advanced) "cifs option modify -max-same-tree-connect-per-session" command.

Syslog Message

Received too many connection requests to the same share from one session: clientIP:port %s:%d, share "%s", user "%s", vserver "%s".

Parameters

IpAddress (STRING): IP address of the client from which multiple share connections have been attempted.
port (INT): Port number of the client from which the TCP connection has been established.
shareName (STRING): Name of the share to which the client is attempting connection.
userName (STRING): User that is attempting to connect to the share.
vserverName (STRING): Vserver associated with this operation.

nblade.cifssametreepersessnotice events

Nblade.cifsSameTreePerSessNotice

Severity

NOTICE

Description

This message occurs when the number of connections to the same share allowed per session nears the configured limit. Upon reaching this limit, any further requests to establish another connection to that share are denied until some connections to the share are released. This typically indicates abnormal client behavior.

Corrective Action

Inspect the application using the connection, and also monitor the other applications on the client. The client might be operating incorrectly due to a faulty application running on it. Rebooting the client might also be helpful. In some cases, clients are operating as expected but require a higher threshold, which you can set by using the (privilege: advanced) "cifs option modify -max-same-tree-connect-per-session" command.

Syslog Message

Received %d connection requests to the same share, nearing the configured limit of %d, from one session: clientIP:port %s:%d, share: "%s", user: "%s", vserver: "%s".

Parameters

currentCount (INT): Current count of the connections on the session.
maxValue (INT): Maximum allowed connections on the session.
IpAddress (STRING): IP address of the client from which multiple share connections have been attempted.
port (INT): Port number of the client from which the TCP connection has been established.
shareName (STRING): Name of the share to which the client is attempting connection.
userName (STRING): User that is attempting to connect to the share.
vserverName (STRING): Vserver associated with this operation.

nblade.cifsshrconnectfailed events

Nblade.cifsShrConnectFailed

Severity

ERROR

Description

This message occurs when the network blade cannot connect to the path specified in the CIFS share.

Corrective Action

Verify that the CIFS share path is valid and that the volume it belongs to is accessible.

Syslog Message

Vserver name: %s, Vserver ID: %d, error description: %s, error code: %d, share name: %s, Windows user name: %s, UNIX user name: %s, server IP address: %s, client IP address: %s.

Parameters

vserverName (STRING): Name for the Vserver associated with this operation.
vserverId (INT): Identifier for the Vserver associated with this operation.
errorDescription (STRING): Description of the error for the CIFS share connection failure.
errorCode (INT): Error code that describes the reason for the CIFS share connection failure.
shareName (STRING): Name of the share to which the connection attempt failed.
domainWinUserName (STRING): Windows domain\user that is attempting to connect to the share.
unixUserName (STRING): UNIX user name.
serverIp (STRING): IP address of the server.
clientIp (STRING): IP address of the client.

nblade.cifswitnessfonotify events

Nblade.cifsWitnessFONotify

Severity

INFORMATIONAL

Description

This message occurs when the Witness system has requested its CIFS clients to move their Continuously Available connections to the local node, due to a failure of the partner node.

Corrective Action

(None).

Syslog Message

The Witness service received a failure notification for the partner node. Notification of %d CIFS clients to move their Continuously Available connections to this node took %d milliseconds to complete.

Parameters

numNotificationsSent (INT): Number of clients notified.
timeTakenInMsecs (INT): Number of milleseconds taken to notify the clients.

nblade.css events

nblade.css.s3.AccessDenied

Severity

ERROR

Description

This message occurs when ONTAP® object-store-server denies access to a user.

Corrective Action

Verify that the user has permission to access the resource. Check access and bucket policy configurations using these commands: 'vserver object-store-server policy show', 'vserver object-store-server policy show-statements', 'vserver object-store-server bucket policy show'.

Syslog Message

Access is denied for user '%s' (Vserver %d), from client IP %s accessing resource '%s'.

Parameters

userName (STRING): Name of the user.
vserverId (INT): ID of the Vserver.
ipAddress (STRING): IP address of the client.
resource (STRING): Resource that the user is trying to access.

nblade.cvo events

nblade.cvo.remote.access

Severity

NOTICE

Description

This message occurs when a remote volume has been accessed in the Cloud Volumes ONTAP® environment.

Corrective Action

(None).

Syslog Message

Detected remote volume access (Vserver: %s) from client IP %s to LIF IP %s. Volume: %s.

Parameters

vserver (STRING): Vserver name.
client_ipaddr (STRING): IP address of the client.
lif_ipaddr (STRING): IP address of the LIF.
volume (STRING): Name of the volume.

nblade.dbladenoresponse events

Nblade.dBladeNoResponse.CIFS

Severity

ERROR

Description

This message occurs when a CIFS network data protocol operation times out because the requesting node cannot communicate with the data-serving node to complete the file operation. If this condition persists, there is likely a problem with the communication between the node that generated the event and the node where the data is located in the cluster.

Corrective Action

Identify the node where the data is located by using the (privilege: advanced) "system node show" command and the UUID of the node. Verify network connectivity between the node that generated the event and the node where the data is located by using the "cluster ping-cluster" and "network ping" commands.

Syslog Message

File operation timed out because there was no response from the data-serving node. Node UUID: %s, file operation protocol: %s.

Parameters

DBladeUuid (STRING): Universally Unique Identifier (UUID) of the node where this operation is trying to access.
protocol (STRING): Network data protocol that timed out while attempting the file operation.

Nblade.dBladeNoResponse.NFS

Severity

ERROR

Description

This message occurs when an NFS network data protocol operation times out because the requesting node cannot communicate with the data-serving node to complete the file operation. If this condition persists, there is likely to be a problem with the communication between the node that generated the event and the node where the data is located in the cluster.

Corrective Action

Identify the node where the data is located by using the (privilege: advanced) "system node show" command and the UUID of the node. Verify network connectivity between the node that generated the event and the node where the data is located by using the "cluster ping-cluster" and the "network ping" commands.

Syslog Message

File operation timed out because there was no response from the data-serving node. Node UUID: %s, file operation protocol: %s, client IP address: %s, Opcode/Procedure: %s(%d).

Parameters

DBladeUuid (STRING): Universally unique identifier (UUID) of the node where this operation is trying to access.
protocol (STRING): Network data protocol that timed out while attempting the file operation.
clientip (STRING): IP address of client that attempted the file operation.
nfsOpcode (STRING): Opcode corresponding to file operation.
fileoperation (INT): File operation during which the timeout happened.

nblade.didnotinitialize events

Nblade.DidNotInitialize

Severity

EMERGENCY

Description

The appliance’s network process failed during initialization due to an internal error (likely there is not enough system memory available to start the necessary kernel threads). Because the network process is not running, file access to volumes on local aggregates is not currently available, and cluster and management virtual interfaces for this appliance are also not currently available.

Corrective Action

Initiate a storage failover (takeover) of any aggregates on this appliance, and perform a "sendhome" operation on these aggregates after this appliance is operational again. Also, verify that data virtual interfaces have properly migrated to another appliance. It is possible that a reboot or a reversion to a known compatible software version could also correct this problem.

Syslog Message

The Network Blade kernel module has failed during initialization.

Parameters

(None).

nblade.ecv events

nblade.ecv.not.ready

Severity

NOTICE

Description

This message occurs when ONTAP® software uses a default Effective Cluster Version (ECV) before the actual ECV has been conclusively determined. Some features might not work as expected until ONTAP can select the correct ECV.

Corrective Action

(None).

Syslog Message

Default ECV %s has been used. The ECV value '%d' does not reflect the cluster’s true ECV status.

Parameters

ecv_variable_name (STRING): Name of the ECV value being used.
ecv_variable_value (INT): ECV value being used.

nblade.execsoverlimit events

nblade.execsOverLimit

Severity

ERROR

Description

This message occurs when a connection has more active requests than the current connection threshold allows to be in flight, resulting in request throttling. Connection performance might be degraded.

Corrective Action

Check the RPC slot setting on the client. Refer to TR-4067 "NFS Best Practice and Implementation Guide" for the recommended value and how to set it.

Syslog Message

The number of in-flight requests from client IP "[%s]:%d" to destination LIF "%s" (Vserver "%d") is greater than the maximum number of in-flight requests allowed (%d). The client might experience degraded performance due to request throttling.

Parameters

clientIpAddress (STRING): IP address of the client.
clientPort (INT): Network port of the client.
lifIpAddress (STRING): IP address of the network interface (LIF).
vserverId (INT): ID of the Vserver.
execsLimit (INT): Maximum number of in-flight requests allowed per connection.

nblade.exportaccesschkfailed events

Nblade.exportAccessChkFailed

Severity

ERROR

Description

This message occurs when the network blade denies access to an exported share when a connection attempt violates an export policy.

Corrective Action

Ensure that the export policy rule for this vserver is defined properly.

Syslog Message

(None).

Parameters

vserverId (INT): Identifier for the vserver associated with this operation.
errorCode (INT): Error code that describes the export access check failure.
shareName (STRING): Name of the share that the user attempted to access.

nblade.exportaccessindeterm events

Nblade.exportAccessIndeterm

Severity

ERROR

Description

This message occurs when client access cannot be evaluated because of an error while matching the client against export rules. Client access might be disrupted due to unresponsive or misconfigured external servers, problems with external server configuration on Data ONTAP®, or internal errors while processing the rules.

Corrective Action

Verify that external name services (such as DNS, NIS, LDAP, Kerberos, or AD) are responsive to queries from Data ONTAP®. Use the "vserver show -fields id" command to get the Vserver name corresponding to Vserver ID, and use the "vol show -fields msid" command to get the volume name corresponding to the volume MSID. Use the "vserver export-policy check-access" command to troubleshoot it further, or contact NetApp technical support for further assistance in reviewing the name services logs.

Syslog Message

Access to volume with MSID %llu in Vserver %u could not be evaluated for client "%s" as per export ruleset %llu.

Parameters

msid (LONGINT): MSID of the volume on which access was attempted.
vserverId (INT): Identifier for the Vserver associated with this access.
clientAddr (STRING): IP address of the client attempting access.
rulesetID (LONGINT): Export rule set ID.

nblade.fcvoldisconnected events

Nblade.fcVolDisconnected

Severity

EMERGENCY

Description

This message occurs when the NFS client attempts to access a FlexCache® volume, but the origin of the FlexCache volume cannot be accessed due to poor network connectivity. As a result, NFS clients will lose access to the FlexCache volume.

Corrective Action

Verify that the FlexCache volume can connect with its origin. If the FlexCache volume and origin volume are on the same cluster, then check the node health by using the "system node show" command. If the FlexCache volume and origin volume are on different clusters, then ensure that the intercluster LIFs on both clusters can connect by using the "network ping" commands to check the connectivity on both the clusters.

Syslog Message

Attempt to access FlexCache volume with MSID %u on Vserver ID %u failed because FlexCache origin volume with MSID %u is not reachable.

Parameters

cacheMsid (LONGINT): MSID of the FlexCache volume.
cacheVserverId (INT): Identifier for the FlexCache Vserver associated with this operation.
originMsid (LONGINT): MSID of the origin of the FlexCache volume.

nblade.fileopenlimitexceeded events

Nblade.fileOpenLimitExceeded

Severity

NOTICE

Description

This message occurs when the number of open files on a single SMB connection or session exceeds the system limit.

Corrective Action

(None).

Syslog Message

Number of open files has reached the maximum limit of (%d).

Parameters

filesopen (INT): Number of files that are open.

nblade.flexcachecaaccess events

Nblade.flexcacheCAAccess

Severity

ERROR

Description

This message occurs when a client tries to access a FlexCache® volume via SMB3 using a continuously available share but is denied because FlexCache does not support persistent handle capability.

Corrective Action

Either remove the continuously available property from the CIFS share or create a new share without this property to access the FlexCache volume over SMB.

Syslog Message

Attempt to access FlexCache volume with MSID %u via SMB3 over a continuously available share is denied.

Parameters

msid (INT): MSID of the FlexCache volume being accessed.

nblade.flexcachevolumeaccess events

Nblade.flexCacheVolumeAccess

Severity

ERROR

Description

This message occurs when a client tries to access a FlexCache volume through an unsupported protocol. Currently only NFSv3 clients are supported by FlexCache.

Corrective Action

Make sure a FlexCache-supported protocol is specified for all client mount operations through which a FlexCache volume can be accessed. If using FlexCache, specify 'nfsvers=3' as an option for the 'mount' command on all clients accessing a FlexCache volume

Syslog Message

Attempt to access FlexCache volume with MSID %u via %s denied.

Parameters

msid (INT): MSID of the FlexCache volume being accessed.
protocol (STRING): Client protocol.

nblade.flexgroupstatefulprotocolaccess events

Nblade.flexgroupStatefulProtocolAccess

Severity

ERROR

Description

This message occurs when the system detects an attempt to use Network Lock Manager (NLM) shared locks on a FlexGroup volume. FlexGroup volumes do not support NLM shared locks.

Corrective Action

FlexGroup volumes do not support shared locks. Consider using FlexGroup volumes that support stateful protocols such as NFSv4.0,NFSv4.1,SMB1 or SMB2 in order to use shared locks.

Syslog Message

Attempt to access FlexGroup volumes with Master Data Set ID "%u" with "%s" is denied.

Parameters

msid (INT): Master Data Set ID of the FlexGroup volume being accessed.
protocol (STRING): Client protocol being used.

nblade.fpolicy events

nblade.fpolicy.extn.failed

Severity

EMERGENCY

Description

This message occurs when an I/O operation directed at a FlexCache® volume fails because the file extension include and exclude list of one of the policies is too long to send to the origin of the FlexCache volume.

Corrective Action

Decrease the number of file extensions configured in the include and exclude list in the FPolicy scope by using the "fpolicy policy scope modify" command.

Syslog Message

FPolicy processing failed on volume MSID "%lu", for Vserver ID "%lu", policy ID "%lu", as the combined length for the file extension include and exclude list is greater than %llu. Decrease the number of file extensions configured.

Parameters

msid (LONGINT): MSID of FlexCache volume.
vserverid (LONGINT): ID of the Vserver.
policyid (LONGINT): ID of the FPolicy.
maxmimumListLengthAllowed (LONGINT): Maximum length that can be sent to the origin volume.

nblade.fpolicy.policy.skip

Severity

EMERGENCY

Description

This message occurs when a non-mandatory FPolicy(tm) policy check is skipped while processing an I/O on the FlexCache® volume because the file extension include and exclude list of the policy is too long to send to the origin volume of the FlexCache volume. The error does not fail the operation and other policies, if any, are matched.

Corrective Action

Decrease the number of file extensions configured in the include and exclude list in the FPolicy scope by using the "fpolicy policy scope modify" command.

Syslog Message

FPolicy check is skipped for a non-mandatory policy ID "%lu" on volume MSID "%lu" for Vserver ID "%lu" because the combined length for the file extension include and exclude list is greater than %llu.

Parameters

policyid (LONGINT): ID of the FPolicy policy.
msid (LONGINT): MSID of the FlexCache volume.
vserverid (LONGINT): ID of the Vserver.
maximumListLengthAllowed (LONGINT): Maximum length that can be sent to the origin volume.

nblade.fpolpassthruconnect events

Nblade.fpolPassthruConnect

Severity

INFORMATIONAL

Description

This message occurs when a pass-through read channel is established between the node and the FPolicy server.

Corrective Action

(None).

Syslog Message

Pass-through read channel with the FPolicy server was established. Vserver ID [%d], FPolicy server IP address [%s].

Parameters

vserverId (INT): Identifier for the Vserver associated with this operation.
fpserverIp (STRING): IP address of the FPolicy server.

nblade.fpolpassthrudisconn events

Nblade.fpolPassthruDisconn

Severity

INFORMATIONAL

Description

This message occurs when the pass-through read channel between the node and the FPolicy server is disconnected.

Corrective Action

(None).

Syslog Message

Pass-through read channel with the FPolicy server is disconnected. Vserver ID [%d], FPolicy server IP address [%s], Disconnect reason [%s].

Parameters

vserverId (INT): Identifier for the Vserver associated with this operation.
fpserverIp (STRING): IP address of the FPolicy server.
disconnReason (STRING): Reason for disconnection.

nblade.fpolpassthruonsmb1 events

Nblade.fpolPassthruOnSMB1

Severity

ERROR

Description

This message occurs during a client attempt to establish an FPolicy pass-through read channel over SMB1, which is not supported.

Corrective Action

Verify that both the client and Data ONTAP® support and are configured for SMB2 or later.

Syslog Message

For Vserver "%s", the FPolicy pass-through read channel request coming from the client "%s" is rejected because it is not supported for SMB1.

Parameters

vserverName (STRING): Vserver associated with this operation.
fpserverIp (STRING): IP address of the client.

nblade.gracebegin events

Nblade.graceBegin

Severity

NOTICE

Description

This message occurs when the NFS server enters the grace state.

Corrective Action

(None).

Syslog Message

NFS server grace state has begun for Vserver "%s", LIF ID "%d", LIP IP address "%s".

Parameters

vserverName (STRING): Vserver Name.
lifId (INT): LIF ID
lifIpAddress (STRING): LIF IP address for the NFS server.

nblade.graceend events

Nblade.graceEnd

Severity

NOTICE

Description

This message occurs when the NFS server exits the grace state.

Corrective Action

(None).

Syslog Message

NFS server grace state has ended for Vserver "%s", LIF ID "%d", LIF IP address "%s".

Parameters

vserverName (STRING): Vserver Name.
lifId (INT): LIF ID
lifIpAddress (STRING): LIF IP address for the NFS server.

nblade.httpmaxconntimeouts events

Nblade.httpMaxConnTimeOuts

Severity

ERROR

Description

This message occurs when the HTTP subsystem, which monitors connection timeouts due to an unresponsive client or data not received from the client within a specified time, especially a PUT request or an HTTP Request containing Request Body. If the number of timeouts allowed in a given period of time is being exceeded, it could be due to network failures or DoS(Denial of Service) attacks. This might result in HTTP client connection failures, because most connections are using resources and waiting for data.

Corrective Action

Inspect the clients that are experiencing a long delay in packet trace tools. Inspecting the client network might be helpful as well.

Syslog Message

The HTTP subsystem on this node on vserver %u has exceeded its connection timeout limit of %llu times, currently %llu connection timeout failures observed since boot time. This might result in unexpected HTTP connection failures.

Parameters

vsId (INT): Id of the vserver, on which this event occurred.
currentNumConnTimeouts (LONGINT): Total number of connection timeouts that occured in the HTTP subsystem.
totalNumConnTimeouts (LONGINT): Maximum number of connection timeouts allowed in the HTTP subsystem.

nblade.httpmemexceeded events

Nblade.httpMemExceeded

Severity

ERROR

Description

This message occurs when the HTTP subsystem, which operates all the HTTP servers exposed through a given node, has requested more memory than it is allowed in this node. The subsystem is restricted to a percentage of total memory in the node, so the node itself need not be low on memory for this to occur. HTTP memory is not allocated in advance and so HTTP memory requests compete with other system processes. This message might not appear if a memory request from HTTP cannot be honored because the node is already low on memory. This might result in HTTP client connection failures.

Corrective Action

Compare the number of memory allocation failures with the previous occurence of this event to understand the load on the system. Further analyze the memory allocated to the HTTP subsystem on this node by viewing the nblade_http object instance for this node through the "statistics show" interface. Based on that data, consider distributing HTTP load by moving data LIFs, adding data LIFs, and redirecting workloads, or by shutting down non-essential workloads to alleviate the memory pressure.

Syslog Message

The HTTP subsystem on this node has exceeded its allotment of %llu bytes of node memory with currently %llu memory allocation failures since boot time. This might result in unexpected HTTP connection failures.

Parameters

availableMemoryInBytes (LONGINT): Amount of memory available to the HTTP subsystem.
memAllocFailures (LONGINT): Number of memory allocation failures in the HTTP subsystem since boot time.

nblade.invtcprecordmarker events

Nblade.invTcpRecordMarker

Severity

ERROR

Description

This message occurs when a TCP connection is reset due to an invalid TCP record marker in an Open Network Computing/Remote Procedure Call request.

Corrective Action

1. Use the IP address from the log to identify the client machine that sent the invalid TCP record marker. 2. Use the TCP port number to determine which service was being requested by the client. 3. Contact the OS vendor for the client machine for a software patch.

Syslog Message

Invalid TCP record marker received from remote IP address %s on local port %d. Vserver ID associated with this operation is %d. Invalid reason is %s, invalid record marker is %d.

Parameters

remoteIpAddress (STRING): IP address of the client machine.
localPort (INT): Local TCP port number that received the data.
VirtualServer (INT): Identifier for the Vserver associated with this operation.
reason (STRING): Reason the record marker was invalid: - "TCP_FRAGMENT" indicates that RPC TCP fragments that are not supported at this time. - "TCP_DATA_LENGTH_OVERFLOW" indicates an oversized record marker; that is, the record marker value was greater than the maximum supported size, currently 1MB. - "TCP_DATA_LENGTH_UNDERFLOW" indicates an undersized record marker; that is, the record marker value was below the minimum supported size, currently 40 bytes.
recordMarker (INT): Actual 32-bit record marker that was received and marked as invalid.

nblade.junctionrootlookup2 events

Nblade.JunctionRootLookup2

Severity

ERROR

Description

This message occurs when the system cannot obtain the root file handle of the volume mounted on a junction path. The cause of the problem might be that the target node is down or the target volume or aggregate is offline. The typical client operation that triggers a junction root lookup is a directory list operation where one of the directory entries is a junction. As long as the root of the volume at the junction cannot be looked up, the NFS client that is listing the directory appears to hang.

Corrective Action

Check whether the volume or aggregate or node that matches the given MSID is offline. If it is, bring it online if possible.

Syslog Message

Junction root lookup of a volume in Vserver %llu with MSID %llu has failed for reason "%s".

Parameters

vserverId (LONGINT): Vserver for this Master Data Set ID (MSID).
msid (LONGINT): MSID of the volume mounted at the junction being looked up.
reason (STRING): Additional information about why the operation failed.

nblade.longrunningrpcop events

Nblade.longRunningRpcOp

Severity

ERROR

Description

This message occurs when a running remote procedure call (RPC) operation takes longer than a defined length of time. The message indicates that the RPC operation has not been completed. If the condition persists, any operation to that RPC server is likely to fail.

Corrective Action

Check the progress of the operation by using the (privilege: advanced) "statistic show -component nblade_rpc_server -instance [RPC_server_name] -raw true -counter curr_head*" command. If the curr_head_proc_time_secs counter keeps incrementing, the operation has not been completed. This condition might cause network configuration and status commands to fail consistently. If the operation does not get completed, contact technical support for assistance.

Syslog Message

Detected a long-running RPC operation (procedure number %u) for RPC server %s. The server has not responded in %lu seconds, which is over the threshold of %lu seconds.

Parameters

procedure (INT): Procedure number of the RPC operation.
RpcServer (STRING): Name of the RPC server.
timeSecs (LONGINT): Time in seconds since the current longest operation was allocated.
timeThresholdSecs (LONGINT): Time threshold that an operation should finish by.

nblade.nbnstoomanylifs events

Nblade.NbnsTooManyLifs

Severity

ERROR

Description

This message occurs when the NetBIOS Name Service receives more than 25 IP addresses for a name registration request. This is typically caused because of an upgrade from a previous release that had more than 25 IP addresses configured for a Vserver and WINS was configured. In such a scenario, clients might not be able to access data because some of the IP addresses might not have registered with WINS.

Corrective Action

If there are more than 25 IP addresses configured for a Vserver, modify the "nbns-enabled-lifs" CIFS option to no more than a maximum of 25 LIFs by using the 'vserver cifs options modify -vserver <vserver> -nbns -enabled-lifs' command in advanced privilege mode when the effective cluster version is Data ONTAP 9.0 or

later. In a mixed-mode cluster with a node running Data ONTAP 8.3, do not configure more than 25 LIFs per Vserver because of the following WINS server limitation: https://www.microsoft.com/resources/documentation/windowsnt/4/server/reskit/en-us/net/sur_wins.mspx

Syslog Message

The NetBIOS Name Service received more than 25 IP addresses for name registration for Vserver %u.

Parameters

vserverId (INT): Identifier for the Vserver associated with this operation.

nblade.newclientidmismatch events

Nblade.NewClientIdMismatch

Severity

ALERT

Description

This message occurs when a namestring collision occurs between NFS clients.

Corrective Action

Ensure client has unique hostname and NFSv4 mount clientaddr to avoid this.

Syslog Message

NFSv4 name string "%s" collision between clients %s and %s.

Parameters

clientNameStr (STRING): Client identifier namestring during SETCLIENTID operation.
existingStr (STRING): IP address of the existing client.
newStr (STRING): IP address of the new client.

nblade.nfs4illegaldirentname events

Nblade.Nfs4IllegalDirentName

Severity

ERROR

Description

This message occurs when a user attempts to list a directory over NFSv4 that contains an entry name with non UTF-8 characters. The problematic directory entry name was most likely created over NFSv2 or NFSv3 and could not be translated to Unicode using the translation table determined by the virtual server's language setting. A possible reason for this could be a client or server language misconfiguration issue.

Corrective Action

Use the "vol show -fields msid" command to find the volume name corresponding to the volume MSID. Use the "volume file show-inode" command with the file ID and volume name information to find the file path. Access the parent directory from an NFSv3 client, and then rename the entry using Unicode characters.

Syslog Message

Directory entry with file ID '%u' on the volume with MSID '%llu' cannot be listed. Directory entry name is illegal for NFSv4.

Parameters

fileid (INT): File ID of the directory entry.
msid (LONGINT): MSID of the volume, where the directory entry resides.

nblade.nfs4opnotsupported events

Nblade.Nfs4OpNotSupported

Severity

NOTICE

Description

This message occurs when a NFSv4 client presents an unsupported operation to the server.

Corrective Action

(None).

Syslog Message

NFSv4 operation '%d' is not supported.

Parameters

opcode (INT): ID of unssupported operation.

nblade.nfs4sequenceinvalid events

nblade.nfs4SequenceInvalid

Severity

NOTICE

Description

This message occurs when an NFS server detects an unexpected value for an incoming sequence number from a client.

Corrective Action

(None).

Syslog Message

NFS client (IP: %s) sent sequence# %d, but server expected sequence# %d. Server error: %s.

Parameters

clientIpAddress (STRING): IP address of the NFS client.
InSeqid (INT): Incoming sequence number from the client.
NextSeqid (INT): Expected sequence number from the server.
NfsError (STRING): NFS protocol error.

nblade.nfsconnresetandclose events

Nblade.nfsConnResetAndClose

Severity

ERROR

Description

This message occurs when the server aborts the connection with the client by sending one or more RST segments, immediately resulting in the connection state being discarded.

Corrective Action

If this message occurs more than three times for a particular client in 30-60 minutes, make note of the IP address of the affected client. Verify that the network between the client and the storage system is functioning normally. After verifying the health of the network, verify that there are no issues related to networking on the client side. Check IP connectivity over the cluster interfaces between the two nodes. If the problem persists after addressing issues on the network or the client, contact NetApp technical support.

Syslog Message

Shutting down connection with the client. Vserver ID is %d; network data protocol is %s, Rpc Xid 0x%x; client IP address:port is %s:%d. local IP address is %s; reason is %s.

Parameters

vserverId (INT): Identifier for the Vserver associated with this operation.
serviceProtocol (STRING): Network data protocol used in the connection.
rpcXid (INT): Remote procedure call XID.
remoteAddr (STRING): IP address of the client machine.
remotePort (INT): TCP or UDP port number used by the remote client to send the data.
localAddr (STRING): IP address of the local interface serving the protocol operation.
reason (STRING): Reason for the disconnection.

nblade.nfscredcacheflushed events

Nblade.nfsCredCacheFlushed

Severity

INFORMATIONAL

Description

This message occurs when the administrator modifies the "extended-groups-limit" option or "auth-sys-extended-groups" option using the "vserver nfs modify" command. This results in the flushing of the entire credential cache, thereby making the subsequent operations slower for a short while until the credential cache is repopulated.

Corrective Action

(None).

Syslog Message

When the administrator modifies the "extended-groups-limit" option or "auth-sys-extended-groups" option using the "vserver nfs modify" command, the entire credential cache is flushed that holds credentials on connections that use mixed-mode security style volumes or RPCSEC_GSS authentication or extended

groups over AUTH_SYS. This makes subsequent operations on such connections slower for a short while, until the credential cache is repopulated. The value of "auth-sys-extended-groups" option is %d (1:enabled, 0:disabled). The value of "extended-groups-limit" option is %d.

Parameters

isExtGroupsEnabled (INT): Flag to indicate if "auth-sys-extended-groups" option is enabled or not.
extendedGroupsLimit (INT): This indicates the number of auxiliary groups supported over RPC security flavors AUTH_SYS or RPCSEC_GSS. The range is 32 to 1024.

nblade.nfsmountrootonly events

Nblade.NfsMountRootOnly

Severity

NOTICE

Description

This message occurs when a non-root user performs MOUNT or NFS operation when the respective options '-mount-rootonly' or 'nfs-rootonly' are enabled.

Corrective Action

(None).

Syslog Message

%s operation by non-root user failed. Vserver ID is %d; ProgramNumber is %d; client IP address:port is %s:%d; local IP address is %s; Procedure number is %d.

Parameters

serviceProtocol (STRING): Network data protocol used in the connection.
vserverId (INT): Identifier for the vserver associated with this operation.
programNumber (INT): RPC Program Number.
remoteAddr (STRING): IP address of the client machine.
remotePort (INT): Remote port number that sent the data.
localAddr (STRING): IP address of the local interface serving the protocol operation.
procedureNum (INT): RPC Procedure Number for the requested operation.

nblade.nfspathresmaxlinks events

Nblade.nfsPathResMaxLinks

Severity

ERROR

Description

This message occurs while resolving an input path, when the server has reached the limit of maximum links it can follow and the corresponding RPC fails.

Corrective Action

Use the client IP address included in this message to identify the client sending the request. An operation such as mount or rquota. failing on this client might be due to this error. Reduce the number of symlinks to be followed for the failing operation.

Syslog Message

NFS maximum symbolic link limit reached when resolving path. Vserver ID: %d, service protocol:version is %s:%d, client IP address:port is %s:%d, local IP address: %s, RPC procedure number: %d.

Parameters

vserverId (INT): Identifier for the Vserver associated with this operation.
serviceProtocol (STRING): Network data protocol used in the connection.
programVersion (INT): RPC program version.
remoteAddr (STRING): IP address of the client machine.
remotePort (INT): Remote port number that sent the data.
localAddr (STRING): IP address of the local interface serving the protocol operation.
procedureNum (INT): RPC procedure number for the requested operation.

nblade.nfsrcchecksummismatch events

Nblade.nfsRCChecksumMismatch

Severity

ALERT

Description

This message occurs when the server detects a retransmitted request from the client with a modified payload. Modified requests from the client could cause corruption and pose a security threat to the server. Please use the information in the event to identify and monitor the bad client connection.

Corrective Action

1. Use the IP address from the log to identify the client machine and connection that retransmitted the invalid modified request. 2. Monitor the client connection and if invalid modified requests are persistent, take steps to ensure the security of the connection has not been compromised. 3. If there are no security concerns with the client connection, then the application driving traffic on that connection and the client OS NFS implementation should be examined to identify potential software defects.

Syslog Message

Replay cache checksum mismatch detected in retransmitted NFS request from client. Vserver ID is %d; service protocol:version is %s:%d, Rpc Xid 0x%x; client IP address:port is %s:%d. local IP address is %s; NFS procedure number is %d.

Parameters

vserverId (INT): Identifier for the vserver associated with this operation.
serviceProtocol (STRING): Network data protocol used in the connection.
programVersion (INT): RPC Program Version.
rpcXid (INT): Remote procedure call XID.
remoteAddr (STRING): IP address of the client machine.
remotePort (INT): Remote port number that sent the data.
localAddr (STRING): IP address of the local interface serving the protocol operation.
procedureNum (INT): RPC Procedure Number for the requested operation.

nblade.nfsv3writetoolarge events

Nblade.Nfsv3WriteTooLarge

Severity

ERROR

Description

This message occurs when a client attempts to write over NFSv3 with an amount of data that is greater than the maximum allowed TCP or UDP transfer size. This is an invalid request from the client and the data is not written.

Corrective Action

Try the operation again with the number of bytes of data that is less than or equal to the maximum allowed TCP or UDP transfer size configured in the server. You can set the write size option in the 'mount' command to the TCP or UDP transfer size.

Syslog Message

%d bytes of data to be written is greater than the maximum allowed TCP or UDP transfer size, which is %d. Data is not written. Associated object type is %s with UUID: %s.

Parameters

opaqueLen (INT): Number of bytes of data that were to be written.
maxXferSize (INT): Maximum allowed TCP/UDP transfer size configured in the server.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the resource object.

nblade.nfsv4nsdbdomainmismatch events

Nblade.Nfsv4NsdbDomainMismatch

Severity

ERROR

Description

This message occurs when an NFSv4 client queries or updates the user or group attribute of a file object but the requested value does not match the '-v4-id-domain' option value of a virtual server’s NFS service. In NFSv4, users and groups are represented as names of the form string@domain. The domain string must match on the client and server to ensure correct operation. The NFSv4 client request, on whose behalf this event message is issued, is rejected with an NFS4ERR_BADOWNER error.

Corrective Action

Update the client or server NFSv4 domain string to ensure that they match. If a single client experiences the issue, you typically just need to modify that client. See the client vendor’s documentation to change the NFSv4 domain name configuration. If multiple clients experience the issue, you typically need to update the value of the '-v4-id-domain' option in the NFS server configuration.

Syslog Message

NFSv4 server %s received domain string %s from client %s, which does not match the '-v4-id-domain' value %s.

Parameters

serverIp (STRING): IP address of the server processing the NFSv4 request.
clientDomain (STRING): NFSv4 domain string received from the client

clientIp (STRING): IP address of the client.
serverDomain (STRING): Domain string that the NFSv4 server expected.

nblade.nfsv4poolexhaust events

Nblade.nfsV4PoolExhaust

Severity

EMERGENCY

Description

This message occurs when one of the NFSv4 store pools is exhausted.

Corrective Action

If the NFS server is unresponsive for more than 10 minutes after this error occurs, contact NetApp technical support.

Syslog Message

NFS Store Pool for %s exhausted. Associated object type is %s with UUID: %s.

Parameters

poolname (STRING): NFSv4 store pool type where the exhaustion happened.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the resource object.

nblade.nfsv4poolthreshold events

Nblade.nfsV4PoolThreshold

Severity

NOTICE

Description

This message occurs when one of the NFSv4 store pools is nearing exhaustion (80% of max size). If the condition is allowed to continue, the store pool limits will be reached leading certain NFSv4 request failures.

Corrective Action

Reduce NFSv4 workload like active opens, users and client connections which consume store pool objects to ensure their counts remain under pre-defined limits.

Syslog Message

NFS Store Pool for %s is nearing exhaustion (%s of pool currently in use).

Parameters

poolname (STRING): NFSv4 store pool type where the maximum limits are nearing.
percent (STRING): Percentage of store pool objects of type currently in use.

nblade.nfsv4writetoolarge events

Nblade.Nfsv4WriteTooLarge

Severity

ERROR

Description

This message occurs when a client attempts to write over NFSv4 with an amount of data that is greater than the maximum allowed TCP transfer size. This is an invalid request from the client and the data is not written.

Corrective Action

Try the operation again with the number of bytes of data that is less than or equal to the maximum allowed TCP transfer size configured in the server. You can set the write size option in the 'mount' command to the TCP transfer size.

Syslog Message

%d bytes of data to be written is greater than the maximum allowed TCP transfer size, which is %d. Data is not written. Associated object type is %s with UUID: %s.

Parameters

opaqueLen (INT): Number of bytes of data that were to be written.
maxtcpxferSize (INT): Maximum allowed TCP transfer size configured in the server.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the resource object.

nblade.nocsmsession events

Nblade.noCsmSession

Severity

NOTICE

Description

This message occurs when the local node could not acquire a Connection Session Manager (CSM) session. CSM sessions are used to communicate file operations between nodes in the cluster. This might be a transient condition. If this condition persists, volumes on the destination node remain unavailable from this node. The destination node can be either local or remote.

Corrective Action

Check IP connectivity over the cluster interfaces between the two nodes. If further assistance is needed, contact NetApp technical support.

Syslog Message

(None).

Parameters

bladeId (STRING): UUID of the node that could not be reached.

nblade.nosmbvernegotiated events

Nblade.noSmbVerNegotiated

Severity

ERROR

Description

This message occurs when Data ONTAP® does not support any of the SMB protocol versions sent by the client for negotiation.

Corrective Action

Ensure that the client supports at least one of the enabled SMB versions. You can determine whether an SMB version is enabled by running the "vserver cifs options show" command in advanced mode.

Syslog Message

For Vserver "%s", Data ONTAP® could not negotiate with the client "%s" because it does not support any of the SMB protocol versions that the client sent in the list "%s".

Parameters

vserverName (STRING): Vserver associated with this operation.
clientIp (STRING): IP address of the client attempting to negotiate.
clientVersionList (STRING): List of the SMB protocol versions sent by the client.

nblade.pcp events

Nblade.pcp.linkThrashing

Severity

INFORMATIONAL

Description

This message occurs when a network port undergoes multiple link state transitions within a short period of time. The event might be triggered in response to a rapid sequence of switch events or there might be a bad link.

Corrective Action

If this problem persists, check the physical connections between the affected port and its network switch. You can identify the faulty port by reviewing the event log for link state transitions reported by the NIC. One or more ports should have reported multiple linkUp and linkDown events prior to the linkThrashing message. ::> event log show -node <node> -messagename netif.link* If checking physical connections does not identify the problem, consider replacing the corresponding NIC.

Syslog Message

Link thrashing detected on port %u.

Parameters

port (INT): Port ID.

nblade.qosvioldetectregfail events

Nblade.QoSViolDetectRegFail

Severity

ERROR

Description

This message occurs when the Quality-of-Service (QoS) subsystem fails to register for updates during initialization due to an internal error (e.g. there is not enough system memory available). As a result, workloads might not meet their minimum throughput or their service-level objectives (SLOs).

Corrective Action

The registration will continue to be retried. If this message continues to occur, perform a planned takeover/giveback sequence to reset the reporting node nondisruptively by using the "takeover -ofnode (reporting_node)" and "giveback -ofnode (reporting_node)" commands. If the problem persists, contact Contact NetApp technical support.

Syslog Message

Failed to register for violation detection updates. QoS min-throughput might operate in a limited capacity.

Parameters

errorCode (INT): Error code that was returned during registration.

nblade.rcbinid events

nblade.RCBinId.timeout

Severity

NOTICE

Description

This message occurs when an NFS replay cache bin ID entry expires.

Corrective Action

(None).

Syslog Message

Found replay cache expired entry for NFS client IP address: %s.

Parameters

ipaddr (STRING): IP address of the NFS client.

nblade.recoverybegin events

Nblade.recoveryBegin

Severity

NOTICE

Description

This message occurs when the NFS server enters the lock recovery state.

Corrective Action

(None).

Syslog Message

NFS server lock recovery has begun for Vserver "%s", LIFID "%d", LIF IP address "%s".

Parameters

vserverName (STRING): Vserver Name.
lifId (INT): LIF ID
lifIpAddress (STRING): LIF IP address for the NFS server.

nblade.scannerconnected events

Nblade.scannerConnected

Severity

NOTICE

Description

This message occurs when a Vserver connects successfully to a Vscan server.

Corrective Action

(None).

Syslog Message

Vserver "%s" connected to Vscan server (IP: %s).

Parameters

vserverName (STRING): Name of the connecting Vserver.
scannerIp (STRING): IP address of the Vscan server.

nblade.scannerdisconnected events

Nblade.scannerDisconnected

Severity

NOTICE

Description

This message occurs when any Vserver disconnects from a Vscan server.

Corrective Action

(None).

Syslog Message

Vserver "%s" disconnected from Vscan server (IP: %s).

Parameters

vserverName (STRING): Name of the disconnected Vserver.
scannerIp (STRING): IP address of the Vscan server.

nblade.sectracequeoverload events

Nblade.sectraceQueOverload

Severity

ALERT

Description

This message occurs when there are too many Sectrace work items. This might be the result of a very generic filter. For example, tracing of succesful NFS accesses can quickly generate a large number of Sectrace items, since all ops (each read or write) might generate a security trace.

Corrective Action

Check the Sectrace filter and make it more specific.

Syslog Message

Too many events [%d] present in SectraceGlobal task queue.

Parameters

queueSize (INT): Number of queued events waiting to be processed.

nblade.sharemaxconnlimit events

Nblade.shareMaxConnLimit

Severity

ERROR

Description

This message occurs when a CIFS share exceeds its maximum configured connection limit.

Corrective Action

Increase the "max-connections-per-share" limit using "vserver cifs share modify" command.

Syslog Message

CIFS share: %s of Vserver: %s hit its maximum connection limit.

Parameters

shareName (STRING): Name of the CIFS share that the user attempted to connect.
vserverName (STRING): Name for the Vserver associated with this operation.

nblade.showmountdisabled events

nblade.showmountdisabled

Severity

ERROR

Description

This message occurs when the "showmount" command is triggered by client, but the command is disabled on the NFS server. The "showmount" command enables NFS clients to see the Vserver’s NFS exports list.

Corrective Action

Use the "nfs modify -showmount enabled" command to enable the feature. Use the "nfs show -fields showmount" command to verify that, if the showmount feature was enabled successfully on the NFS server.

Syslog Message

Showmount is disabled on Vserver %d.

Parameters

vserverid (INT): Identifier for the Vserver associated with this operation.

nblade.smb1onlyclientfound events

Nblade.smb1OnlyClientFound

Severity

NOTICE

Description

This message occurs when ONTAP® detects a client that supports only the SMB1 protocol. This message can help in identifying such clients and preparing for their upgrade to SMB2 or later before ONTAP deprecates the SMB1 version of the protocol.

Corrective Action

(None).

Syslog Message

For Vserver "%s", Data ONTAP® detected a client "%s" that supports only the SMB1 version of the protocol.

Parameters

vserverName (STRING): Vserver associated with this operation.
clientIp (STRING): IP address of the client.

nblade.smbsignaturemismatch events

Nblade.smbSignatureMismatch

Severity

ERROR

Description

This message occurs when the SMB signature sent by client does not match the SMB signature generated by the CIFS server.

Corrective Action

Ensure that the SMB client is authenticated in order to access the files. Alternatively, disable SMB signing.

Syslog Message

Client (protocol dialect: %s, IP: %s) sent an SMB signature that does not match the signature generated by the CIFS server: %s (Vserver: %s).

Parameters

SmbDialect (STRING): SMB protocol dialect negotiated by the client.
IpAddress (STRING): IP address of the client.
CifsServerName (STRING): Cifs server name of the client.
VserverName (STRING): Vserver name.

nblade.testevent events

Nblade.TestEvent

Severity

INFORMATIONAL

Description

This is a test EMS event generated by the Network Blade for functional verification only. No action is required.

Corrective Action

No corrective action is required. If this message is appearing without being intentionally triggered by the customer or by support activity, please contact support.

Syslog Message

The Network Blade kernel module has generated a test EMS event.

Parameters

(None).

nblade.vifdel events

Nblade.vifdel.ipRemoveFailed

Severity

ERROR

Description

This message occurs when there is a failure removing the IP address of a LIF that is being deleted. While this condition persists, most networking configuration or status operations can not be performed.

Corrective Action

A system reboot may be required if the operation did not complete successfully after it was retried. For HA configurations, operational disruption can be minimized by initiating a partner takeover followed by a reboot of this partner. After the reboot is complete, issue a "giveback" command to return services to this partner.

Syslog Message

Error deleting IP address from LIF %d, error %d.

Parameters

lif (INT): LIF Id.
error (INT): Operation error code.

Nblade.vifdel.longRunning

Severity

ERROR

Description

This message occurs when there is an excessive delay in removing connections before LIF deletion can be completed. While this condition persists, most networking configuration or status operations can not be performed.

Corrective Action

A system reboot may be required if this message has occurred multiple times for the same LIF and the number of connections remaining has not decreased across these messages. In addition, network configuration and status commands are still not working. For HA configurations, operational disruption can be minimized by initiating a partner takeover followed by a reboot of this partner. Prior to reboot or takeover, a full autosupport must be generated for the affected node. This is done via the "autosupport invoke -type full" command. If possible, a sync core of the affected node should be provided to help find the root cause. A sync core can be generated via the "reboot -dump true" command for the affected node. After the reboot is complete, issue a "giveback" command to return services to this partner for HA configurations.

Syslog Message

Excessive delay while deleting connections on LIF %d, %d connections remaining.

Parameters

lif (INT): LIF Id.
remainingConns (INT): Number of connections still remaining on this LIF.

nblade.vldb events

Nblade.vldb.LeakedBladeList

Severity

ALERT

Description

This message occurs when a protocol requests a list of blades, the current blade list is too old, and a new list needs to be generated. However, one or more references given to the previous requests has not yet been released.

Corrective Action

To restore proper operation of the affected protocol, a reboot of the node will be required. Rebooting the node with the "system node reboot -dump true" command saves a core dump that allows diagnosis of this issue by NetApp technical support. For more information or assistance, contact NetApp technical support.

Syslog Message

%s operation issued by %s on cached VLDB blade list with references pending beyond expiry time.

Parameters

operation (STRING): Type of operation the caller is attempting.
caller (STRING): Caller that is trying to perform the operation.

Nblade.vldb.Timeout

Severity

ERROR

Description

This message occurs when a request from the network module to the volume location database (VLDB) times out. The VLDB is used to identify the node that currently controls a volume. This might be a transient condition. If the condition persists, some volumes might be inaccessible.

Corrective Action

Contact NetApp technical support.

Syslog Message

Request from the network module to the volume location database (VLDB) timed out.

Parameters

(None).

nblade.vscanbadipprivaccess events

Nblade.vscanBadIPPrivAccess

Severity

ERROR

Description

This message occurs during a client attempt to connect to the privileged ONTAP_ADMIN$ share, when the IP address of that client is not found in the list of allowed IP addresses.

Corrective Action

Ensure that the mentioned IP address is configured in one of the active vscan scanner pools. Use the "vserver vscan scanner pool show-active" command to view the currently active scanner pool configuration.

Syslog Message

For Vserver "%s", the attempt to connect to the privileged ONTAP_ADMIN$ share by the client "%s" is rejected because its IP or hostname is not configured in any of the Vserver active scanner pools.

Parameters

vserverName (STRING): Vserver associated with this operation.
scannerIp (STRING): IP address of the client.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the resource object.

nblade.vscanbadprotomagicnum events

Nblade.vscanBadProtoMagicNum

Severity

ERROR

Description

This message occurs when an incorrectly formatted message is received from the AV Connector. This might result in delay or failure in AV scanning.

Corrective Action

Ensure that the compatible version of AV Connector is running on the AV server, and that no other user or software is attempting to connect to the "\\PIPE\vscan" resource on the Vserver.

Syslog Message

Data ONTAP® received incorrectly formatted message for Vserver "%s" from AV Connector running on the AV server "%s".

Parameters

vserverName (STRING): Vserver associated with this operation.
scannerIp (STRING): IP address of the AV server.

nblade.vscanbaduserprivaccess events

Nblade.vscanBadUserPrivAccess

Severity

ERROR

Description

This message occurs during a client attempt to connect to the privileged ONTAP_ADMIN$ share, when the logged-in user of that client is not found in the list of allowed users.

Corrective Action

Ensure that the mentioned user name and IP address is configured in one of the active vscan scanner pools. Use the "vserver vscan scanner pool show-active" command to view the currently active scanner pool configuration.

Syslog Message

For Vserver "%s", the attempt to connect to the privileged ONTAP_ADMIN$ share by the client "%s" is rejected because its logged-in user "%s" is not configured in any of the Vserver active scanner pools.

Parameters

vserverName (STRING): Vserver associated with this operation.
scannerIp (STRING): IP address of the client.
userName (STRING): Logged-in user of the client.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the resource object.

nblade.vscanconnbackpressure events

Nblade.vscanConnBackPressure

Severity

ERROR

Description

This message occurs when an AV server is too busy to accept new scan requests.

Corrective Action

If this message occurs frequently, ensure that there are enough AV servers to handle the virus-scanning load being generated by the mentioned Vserver.

Syslog Message

For Vserver "%s", AV server "%s" is too busy to accept new scan requests.

Parameters

vserverName (STRING): Vserver associated with this operation.
scannerIp (STRING): IP address of the AV server.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the resource object.

nblade.vscanconninactive events

Nblade.vscanConnInactive

Severity

NOTICE

Description

This message occurs when ONTAP® detects a nonresponsive antivirus (AV) server and forcibly closes its vscan connection.

Corrective Action

Ensure that the AV Connector, installed on the AV server, can connect to the Vserver and receive the scan requests.

Syslog Message

For Vserver "%s", ONTAP® forcibly closed the vscan connection originated from the nonresponsive AV server "%s".

Parameters

vserverName (STRING): Vserver associated with this operation.
scannerIp (STRING): IP address of the AV server.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the resource object.

nblade.vscanconninvaliduser events

Nblade.vscanConnInvalidUser

Severity

NOTICE

Description

This message occurs during a client attempt to establish a vscan connection, when the logged-in user of that client is not found in the list of allowed users.

Corrective Action

Ensure that the mentioned user name is configured in one of the active vscan scanner pools. Use the "vserver vscan scanner pool show-active" command to view the currently active scanner pool configuration.

Syslog Message

For Vserver "%s", the vscan connection request coming from client "%s" is rejected because the logged-in user "%s" is not configured in any of the Vserver active scanner pools.

Parameters

vserverName (STRING): Vserver associated with this operation.
scannerIp (STRING): IP address of the client attempting to establish a vscan connection.
userName (STRING): User name of the client attempting to establish a vscan connection.

nblade.vscanconnreqonsmb1 events

Nblade.vscanConnReqOnSMB1

Severity

ERROR

Description

This message occurs during a client attempt to establish a vscan connection over SMB1, which is not supported.

Corrective Action

Verify that both the client and Data ONTAP® support and are configured for SMB2 or later.

Syslog Message

For Vserver "%s", the vscan connection request coming from the client "%s" is rejected because it is not supported for SMB1.

Parameters

vserverName (STRING): Vserver associated with this operation.
scannerIp (STRING): IP address of the client.

nblade.vscannodispatcher events

Nblade.vscanNoDispatcher

Severity

ALERT

Description

This message occurs when the vscan-dispatcher component cannot be created. This might be due to internal errors on the system, such as nonavailability of memory. This might cause data unavailability if the scan-mandatory option is enabled.

Corrective Action

Disable Vscan and enable it again by using the "vserver vscan disable/enable" command. If the problem persists, contact NetApp technical support.

Syslog Message

Vscan dispatcher component for Vserver "%s" could not be created. Error: %d.

Parameters

vserverName (STRING): Vserver associated with this operation.
errorCode (INT): Error code that describes the reason for the failure.

nblade.vscannopolicyenabled events

Nblade.vscanNoPolicyEnabled

Severity

ALERT

Description

This message occurs when a file access is not considered for virus scanning because none of the configured On-Access policies are enabled for the Vserver.

Corrective Action

Enable one of the configured On-Access policies for the Vserver.

Syslog Message

For Vserver "%s", the file access was not considered for virus scanning because none of the configured On-Access policies are enabled.

Parameters

vserverName (STRING): Vserver associated with this operation.

nblade.vscannoregdscanner events

Nblade.vscanNoRegdScanner

Severity

ERROR

Description

This message occurs when AV Connector notifies ONTAP® that it does not have a registered scan-engine. This could happen if the scan-engine never registered or unregistered because of some reason like it is misconfigured or shutdown. This might cause data unavailability if the scan-mandatory option is enabled.

Corrective Action

Ensure that the scan-engine software installed on the AV server is compatible with ONTAP®. Also ensure that it is running and is configred to connect to the AV Connector over local loopback.

Syslog Message

For Vserver "%s", AV Connector running on the AV server "%s" does not have a registered scan-engine to it.

Parameters

vserverName (STRING): Vserver associated with this operation.
scannerIp (STRING): IP address of the AV server.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the resource object.

nblade.vscannoscannerconn events

Nblade.vscanNoScannerConn

Severity

EMERGENCY

Description

This message occurs when ONTAP® has no vscan connection for servicing virus scan-requests. This might cause data unavailability if the scan-mandatory option is enabled.

Corrective Action

Ensure that the scanner pool is properly configured and the AV servers are active and connected to ONTAP.

Syslog Message

Vserver "%s" has no virus scanner connection.

Parameters

vserverName (STRING): Vserver associated with this operation.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the resource object.

nblade.vscanvirusdetected events

Nblade.vscanVirusDetected

Severity

ERROR

Description

This message occurs when a vscan server reports an error to the storage system. Normally this indicates that a virus has been found by the vscan server; however, other error conditions on the vscan server can result in this event. Client access to the file is denied. The vscan server might, depending on its settings and configuration, clean the file, quarantine it, or delete it.

Corrective Action

Check the log of the vscan (antivirus) server reported in the syslog message to see if it was able to successfully quarantine or delete the infected file. If it was not able to do so, a system administrator might want to manually delete the file.

Syslog Message

Possible virus detected. Vserver: %s, vscan server IP: %s, file path: %s, client IP: %s, SID: %s, vscan engine status: %u, vscan engine result string: %s.

Parameters

vserverName (STRING): Name of the Vserver associated with this operation.
vscanServerIp (STRING): IP address of the vscan server.
filePath (STRING): Path of the file that was found to be infected.
clientIp (STRING): IP address of the client.
SID (STRING): SID of the client.
vscanEngineStatus (INT): Status code returned by the vscan server.
vscanEngineResultString (STRING): Result string returned by the vscan server.
object_type (STRING): Type of the resource object under notification.
object_uuid (STRING): UUID of the resource object.

nblade.vscanworkqueueoverloaded events

Nblade.vscanWorkQueueOverloaded

Severity

NOTICE

Description

This message occurs when there are too many events being generated by the Vscan subsystem in ONTAP® software, which might be the result of a misconfigured Vscan server.

Corrective Action

Check the Vscan server configurations to make sure that there are no connectivity or configuration issues between the storage system and Vscan server. Use the "vserver vscan connection-status show-all" command to see the connection states of all configured Vscan servers.

Syslog Message

Too many events [%d] present in Vscan work queue.

Parameters

workQueueDepth (INT): Number of queued events waiting to be processed.

Copyright information

Trademark information