secd events

ONTAP 9.15.1 EMS reference

NetApp
June 10, 2024

Table of Contents

secd events

secd.asidtrans events

secd.asidTrans.invalidAsid

Severity

ALERT

Description

This message occurs when ONTAP® software cannot translate an abbreviated SID to a Windows SID. An abbreviated SID is an internal ID maintained by ONTAP. This failure can cause CIFS share access issues.

Corrective Action

Contact NetApp technical support.

Syslog Message

For Vserver "%s", ONTAP could not translate an abbreviated SID to a Windows SID.

Parameters

vserverName (STRING): Vserver associated with this operation.

secd.authsys events

secd.authsys.lookup.failed

Severity

ERROR

Description

This message occurs when the incoming UNIX user ID (UID) that tries to mount or access a mount point cannot be looked up in any of the name-services (NIS, LDAP, file).

Corrective Action

Ensure that the UNIX UID that is trying to mount or access a mount point is part of a name-service, such as NIS, LDAP, or file.

Syslog Message

Unable to retrieve credentials for UNIX user with UID (%u) on Vserver (%s) for client with IP address (%s).

Parameters

uid (INT): UNIX UID.
vserverName (STRING): Name of the Vserver.
clientIP (STRING): IP Address of the client.

secd.cifs events

secd.cifs.machacct.missing

Severity

ALERT

Description

This message occurs when the CIFS server machine account is missing from the Active Directory domain.

Corrective Action

Create the missing CIFS server machine account in Active Directory under the appropriate domain and organizational unit. Then run "vserver cifs password-change" command to begin using it.

Syslog Message

The CIFS server machine account '%s' for Vserver '%s' is missing from the Active Directory domain '%s'.

Parameters

acctName (STRING): Name of the missing CIFS server machine account.
vserverName (STRING): Vserver whose CIFS server machine account is missing.
domainName (STRING): Name of the Active Directory domain.

secd.cifsauth events

secd.cifsAuth.denied

Severity

ERROR

Description

This message occurs when a CIFS authentication attempt fails for any reason other than an unknown user name or bad password.

Corrective Action

Examine the failure details to determine corrective action. A common failure is the inability to communicate with a domain controller.

Syslog Message

vserver (%s) Cannot authenticate CIFS user. %s

Parameters

vserverName (STRING): vserver associated with this operation.
failureDetail (STRING): Error journal is a collection of events leading up to a failure. This failure is likely to impact many (if not all) users, and might reflect a misconfiguration or environmental problem..

secd.cifsAuth.noNameMap

Severity

ERROR

Description

This message occurs when a CIFS authentication succeeds, but system cannot map the Windows user to an appropriate UNIX user.

Corrective Action

Examine the failure details to determine corrective action. Common failures include no appropriate Windows-to-UNIX name mapping rules, no configured default UNIX user, or the inability of the system to communicate with NS-SWITCH authorization sources.

Syslog Message

vserver (%s) CIFS name to UNIX name mapping problem. %s

Parameters

vserverName (STRING): vserver associated with this operation.
failureDetail (STRING): Error journal is a collection of events leading up to a failure. This failure is likely to impact many (if not all) users, and might reflect a misconfiguration or environmental problem..

secd.cifsAuth.noUnixCreds

Severity

ERROR

Description

This message occurs when the system is unable to retrieve necessary UNIX credentials for a Windows user during the CIFS authentication process.

Corrective Action

Examine the failure details to determine corrective action. A common failure is the inability to communicate with NS-SWITCH authorization sources.

Syslog Message

vserver (%s) Cannot get UNIX credentials for CIFS user. %s

Parameters

vserverName (STRING): vserver associated with this operation.
failureDetail (STRING): Error journal is a collection of events leading up to a failure. This failure is likely to impact many (if not all) users, and might reflect a misconfiguration or environmental problem..

secd.cifsAuth.problem

Severity

ERROR

Description

This message occurs when a CIFS authentication attempt fails for any reason other than an unknown user name or bad password.

Corrective Action

Examine the failure details to determine corrective action. Common failures include the inability to communicate with domain controllers, NIS servers, or LDAP servers due to connectivity or configuration problems.

Syslog Message

vserver (%s) General CIFS authentication problem. %s

Parameters

vserverName (STRING): vserver associated with this operation.
failureDetail (STRING): Error journal is a collection of events leading up to a failure. This failure is likely to impact many (if not all) users, and might reflect a misconfiguration or environmental problem..

secd.conn events

secd.conn.auth.failure

Severity

NOTICE

Description

This message occurs when the Vserver cannot establish a TCP/UDP connection to or be authenticated by an outside server such as NIS, LSA, LDAP and KDC. Subsequently, some features of the storage system relying on this connection might not function correctly.

Corrective Action

Ensure that the server being accessed is up and responding to requests. Ensure that there are no networking issues stopping the Vserver from communicating with this server. If the error reported is related to an authentication attempt, ensure that any related configurable user credentials are set correctly.

Syslog Message

Vserver (%s) could not %s over the network to server (%s)%s. Error: %s (%s).

Parameters

vserverName (STRING): Vserver associated with this operation.
connAuthAttempt (STRING): Connection or authentication attempt.
serverInfo (STRING): Name or IP:Port of the server that was related to the failure.
sourceInfo (STRING): Information about the source that was making the connection or authentication.
ErrnoMessage (STRING): Errno message from the connection or authentication failure.
operation (STRING): Operation being performed.

secd.dc events

secd.dc.out.of.pipe.instances

Severity

ALERT

Description

This message occurs when the Windows Domain Controller (DC), while responding to an MSRPC request from Data ONTAP®, returns an error indicating that it ran out of pipe instances in the listening state. This can happen when the requests from Data ONTAP are received by the DC during a timing window when the limited number of listening pipe instance are already allocated to other requests. Such errors received by Data ONTAP might result in longer CIFS/NFS authentication and/or access times, potentially resulting in CIFS/NFS client timeouts.

Corrective Action

Contact Microsoft support.

Syslog Message

MSRPC for Vserver %s to %s:%s was retried %d times (delay: %d usecs).

Parameters

vserver (STRING): Vserver that encountered the failure.
dc (STRING): DC that returned the error.
pipe (STRING): Pipe on the DC.
retries (INT): Number of retries.
delay (INT): Time (usecs) spent retrying.

secd.dns events

secd.dns.server.timed.out

Severity

ERROR

Description

This message occurs when the DNS server fails to respond to a query and timeout occurs.

Corrective Action

Make sure that the DNS server is up and running and that there are no networking issues preventing the Vserver from communicating with the DNS server.

Syslog Message

DNS server %s did not respond to vserver = %s within timeout interval.

Parameters

ipaddr (STRING): Ip address of the DNS server.
vsName (STRING): Name of the Vserver for which DNS response timed out.

secd.dns.srv.lookup.failed

Severity

ERROR

Description

This message occurs when the Domain Name Service (DNS) server fails to look up a service name.

Corrective Action

Make sure that the service name is input correctly and that there are no networking issues preventing the Vserver from communicating with the DNS server.

Syslog Message

DNS server failed to look up service (%s) for vserver (%s) with error (%s).

Parameters

serviceName (STRING): Service name to look up.
vsName (STRING): Name of the Vserver.
errorMsg (STRING): Error message of the failure.

secd.ipq events

secd.ipq.invalid.entry

Severity

ERROR

Description

This message occurs when the IP qualified name-mapping entry is omitted because of an error during the name-mapping check. For example, an error can occur if a host name is configured as the value for ip-qualifier but the hostname lookup fails, in combination with no IP address defined in the name-mapping configuration to validate against the incoming user.

Corrective Action

After resolving the error reported in this message, run the "vserver name-mapping refresh-hostname-ip" command to refresh the name-mapping information.

Syslog Message

Skipping the name-mapping entry on Vserver "%s" for user "%s" at position %u. Reason: %s.

Parameters

vserverName (STRING): Vserver associated with this operation.
userName (STRING): Name of the user.
position (INT): Name-mapping position.
errorString (STRING): Description of the specific error condition: for example, "Failed to lookup hostname gpo.co.in."

secd.kerberos events

secd.kerberos.clockskew

Severity

ERROR

Description

This message occurs when there is a "time error"(clock skew, time skew, time out of bounds). This error indicates that there is a time discrepancy between client and node or client and Key Distribution Center (KDC). The Kerberos authentication request from the client or the node was forwarded to the KDC and it failed because the timestamp encrypted in the Kerberos ticket was different by more than the maximum time difference that is configured on the KDC.

Corrective Action

Ensure that the clock time of the node is identical to that of the client and to that of the KDC. To keep the node and KDC time clocks in synchronization automatically, configure Network Time Protocol (NTP) services on the node. Increasing the clock skew interval may also alleviate this condition: To do so, modify the Kerberos-realm configuration clock-skew parameter (denoted as "Maximum tolerance for computer clock synchronization" in Windows® Active Directory) from the default 300 seconds to 600 seconds or more. Note: Increasing the clock-skew interval makes the client protocols less secure against network replay attacks.

Syslog Message

Kerberos client or node clock skew error for vserver (%s)%s

Parameters

vserverName (STRING): Name of the vserver that is having the error.
clientInfo (STRING): Information of the client that is having the error if available.

secd.kerberos.lookupFailed

Severity

ERROR

Description

This message occurs when the Kerberos user is not a part of any name-service. ONTAP maps the Kerberos Service Principal Name(SPN) to a NFS user name while establishing a security context. If the NFS user name is not found in any of the name-services (LDAP, NIS, file), it leads to a failure in establishing security context, which in turn fails the Kerberos mount.

Corrective Action

Ensure that there is a corresponding UNIX user name for the Kerberos Service Principal Name(SPN) in name services such as NIS, LDAP, or file.

Syslog Message

Unable to map Kerberos user (%s) to appropriate UNIX user on Vserver (%s).

Parameters

uname (STRING): Kerberos NFS user.
vserverName (STRING): Name of the Vserver.

secd.kerberos.noAuthdata

Severity

ERROR

Description

This message occurs when a Kerberos ticket for a user does not contain authorization data.

Corrective Action

Ask the user to obtain a new, valid Kerberos ticket and map the share again.

Syslog Message

Kerberos client has no authorization data for Vserver "%s" with user account "%s".

Parameters

vserverName (STRING): Name of the Vserver on which the error occurred.
userAccount (STRING): User account for which there is insufficient credential information.

secd.kerberos.preauth

Severity

ERROR

Description

This message occurs when invalid credentials are provided for an Active Directory user or the machine account password is out of sync with the credentials set in the Active Directory.

Corrective Action

If the reported error is due to invalid credentials, make sure valid credentials are provided for the Active Directory user. Otherwise, if the reported error is due to an out-of-sync machine account password, run the "vserver cifs password-reset -vserver vserver_name" command to update the password in the Active Directory.

Syslog Message

A Kerberos pre-authentication failure occurred for SVM "%s" due to %s.

Parameters

vserverName (STRING): Name of the storage VM (SVM) that is having the error.
errReason (STRING): Reason for the pre-authentication error.

secd.kerberos.tktexpired

Severity

ERROR

Description

This message occurs when the client’s ticket has expired. This error indicates that the timestamp encrypted in the client’s Kerberos ticket has exceeded it’s maximum lifetime or expired.

Corrective Action

Ensure that the clock time of the node is identical to that of the client and to that of the KDC. To keep the node and KDC time clocks in synchronization automatically, configure Network Time Protocol (NTP) services on the node. Increasing the clock skew interval may also alleviate this condition: To do so, modify the Kerberos-realm configuration clock-skew parameter (denoted as "Maximum tolerance for computer clock synchronization" in Windows® Active Directory) from the default 300 seconds to 600 seconds or more. Note: Increasing the clock-skew interval makes the client protocols less secure against network replay attacks.

Syslog Message

Kerberos client ticket has expired for vserver (%s)%s

Parameters

vserverName (STRING): Name of the vserver that is having the error.
clientInfo (STRING): Information of the client that is having the error if available.

secd.kerberos.tktnyv

Severity

ERROR

Description

This message occurs when the client presented a ticket to the server that is not yet valid (in relationship to the server time). This error indicates that the clocks on the KDC and the client are not synchronized.

Corrective Action

Ensure that the clock time of the node is identical to that of the client and to that of the KDC. To keep the node and KDC time clocks in synchronization automatically, configure Network Time Protocol (NTP) services on the node. Increasing the clock skew interval may also alleviate this condition: To do so, modify the Kerberos-realm configuration clock-skew parameter (denoted as "Maximum tolerance for computer clock synchronization" in Windows® Active Directory) from the default 300 seconds to 600 seconds or more. Note: Increasing the clock-skew interval makes the client protocols less secure against network replay attacks.

Syslog Message

Kerberos client ticket not yet valid for vserver (%s)%s

Parameters

vserverName (STRING): Name of the vserver that is having the error.
clientInfo (STRING): Information of the client that is having the error if available.

secd.ldap events

secd.ldap.bindDn.missing

Severity

ALERT

Description

This message occurs when the -bind-dn user is not configured and the -bind-as-cifs-server option is set to false in the Lightweight Directory Access Protocol (LDAP) client configuration. This LDAP configuration is not recommended because it might result in CIFS credentials being used for authentication if CIFS configuration is present (even though -bind-as-cifs-server is not set). It might also result in anonymous authentication attempts.

Corrective Action

Configure the bind distinguished name (user) and the bind user’s password using the following commands: vserver services name-service ldap client modify -bind-dn vserver services name-service ldap client modify-bind-password

Syslog Message

The LDAP bind DN user is not configured on Vserver %s.

Parameters

vserverName (STRING): Vserver associated with this operation.

secd.ldap.conn.waitTimeout

Severity

ALERT

Description

This message occurs when a connection could not be attempted to any of the configured Lightweight Directory Access Protocol (LDAP) servers. Usually, this issue is seen when the LDAP servers are slow to respond to previous connection requests and SecD has reached the maximum number of simultaneous connection requests. This issue can result in longer CIFS/NFS access times, potentially resulting in client failures or timeouts.

Corrective Action

From an LDAP client workstation, ensure that all configured LDAP servers are responding to requests. Ensure that networking issues do not prevent the cluster from communicating with the servers.

Syslog Message

Connection could not be attempted to the LDAP servers configured on SVM "%s" for LDAP service type (%s) because SecD has exceeded the maximum number of simultaneous connection requests.

Parameters

vserverName (STRING): Storage virtual machine (SVM) associated with this operation.
ldapOperation (STRING): LDAP operation and service for which the connection is required.

secd.ldap.connectFailure

Severity

ALERT

Description

This message occurs when the server could not establish a TCP connection to a Lightweight Directory Access Protocol (LDAP) server.

Corrective Action

From a LDAP client workstation, make sure that the LDAP server is responding to requests. Also make sure that the portmapper on the LDAP server is responding to requests. Make sure that there are no networking issues stopping the cluster from communicating with this LDAP server.

Syslog Message

vserver (%s) could not make a connection over the network to LDAP server (%s) at address (%s) and received error (%s)

Parameters

vserverName (STRING): vserver associated with this operation.
serverName (STRING): Name of the LDAP server that was not responding.
serverAddress (STRING): Address of the LDAP server that was not responding.
ldaperror (STRING): Internal LDAP client library error.

secd.ldap.hostnames.not.resolved

Severity

ERROR

Description

This EMS is generated when none of the configured LDAP hostnames can be resolved.

Corrective Action

Examine the DNS configuration for the corresponding Vserver.

Syslog Message

None of the hostnames can be resolved for Vserver: %s.

Parameters

vserverName (STRING): Vserver associated with this operation.

secd.ldap.hostnames.resolved.partially

Severity

ERROR

Description

This EMS is generated when some of the configured LDAP hostnames cannot be resolved.

Corrective Action

Examine the DNS configuration for the corresponding Vserver.

Syslog Message

Hostnames cannot be resolved for Vserver: %s, unresolvedHosts: %s.

Parameters

vserverName (STRING): Vserver associated with this operation.
unresolvedHostnames (STRING): Hostnames which cannot be resolved.

secd.ldap.noServers

Severity

EMERGENCY

Description

This message occurs when none of the configured Lightweight Directory Access Protocol (LDAP) servers are accepting connections.

Corrective Action

From an LDAP client workstation, make sure that all configured LDAP servers are responding to requests. Ensure that there are no networking issues stopping the cluster from communicating with the configured LDAP servers. Also, ensure that the portmapper running on the LDAP server is working correctly.

Syslog Message

None of the LDAP servers configured for Vserver (%s) are currently accessible via the network for LDAP service type (%s).

Parameters

vserverName (STRING): Vserver associated with this operation.
ldapOperation (STRING): LDAP operation and service for which the connection is required.

secd.ldap.query.timed.out

Severity

ERROR

Description

This message occurs when the LDAP server fails to respond to a query and timeout occurs.

Corrective Action

Because LDAP server timeouts might be the result of connectivity issues between the storage controller and the external service or latency in LDAP server response time, ensure that external connectivity and external services have not been disrupted.

Syslog Message

Vserver '%s': LDAP server %s did not respond to query within timeout (%d seconds) interval.

Parameters

vsName (STRING): Name of the Vserver for which LDAP response timed out.
ipaddr (STRING): IP address of the LDAP server.
timeout (INT): Number of seconds before the LDAP query is timed out.

secd.ldap.referralError

Severity

INFORMATIONAL

Description

This message indicates that the domain controller does not have a copy of the requested object (which exists) and it is providing a location that is more likely to hold the object.

Corrective Action

Modify the environment to avoid LDAP referrals.

Syslog Message

Server (%s) does not hold the target entry for ldap filter (%s) on vserver (%s).

Parameters

serverAddress (STRING): Address of the LDAP server that responded with referral.
ldapSearchFilter (STRING): The Ldap search filter associated with this operation.
vserverName (STRING): Vserver associated with this operation.

secd.ldap.sasl.bind.delayed

Severity

ERROR

Description

This message occurs when a Lightweight Directory Access Protocol (LDAP) server responds slowly to SASL bind requests. This might result in longer SMB/CIFS authentication times, potentially resulting in SMB/CIFS client timeouts. Also, this might affect other LDAP bind requests and Security Daemon (SecD) delays.

Corrective Action

Ensure that there are no networking issues creating intermittent communication problems with the LDAP server. Make sure that the machine running LDAP is responsive and not overloaded.

Syslog Message

LDAP SASL bind taking longer time on server "%s" for SVM "%s".

Parameters

serverAddress (STRING): Address of the LDAP server that is not responding fast enough.
vserverName (STRING): SVM associated with this operation.

secd.ldap.slowServer

Severity

ERROR

Description

This message indicates that the Lightweight Directory Access Protocol (LDAP) server is not responding to requests in the expected time frame.

Corrective Action

Make sure that there are no networking issues creating intermittent communication problems with the LDAP server. Make sure that the machine running LDAP is responsive and not overloaded. From a LDAP client workstation, run LDAP commands to verify long response times.

Syslog Message

from CIFS Server(%s) calls to LDAP server (%s) at address (%s) is executing slowly enough to adversely impact the performance of your server.

Parameters

vserverName (STRING): vserver associated with this operation.
serverName (STRING): Name of the LDAP server that was not responding fast enough.
serverAddress (STRING): Address of the LDAP server that was not responding fast enough.

secd.ldap.starttls.delayed

Severity

ERROR

Description

This message occurs when Lightweight Directory Access Protocol (LDAP) server responses to STARTTLS requests take 5 or more seconds. This might result in longer SMB/CIFS authentication times, potentially resulting in SMB/CIFS client timeouts. Also, this might affect other LDAP bind requests and Security Daemon (SecD) delays.

Corrective Action

Ensure that there are no networking issues creating intermittent communication problems with the LDAP server. Make sure that the machine running LDAP is responsive and not overloaded.

Syslog Message

The STARTTLS operation is taking too long on LDAP server "%s" for SVM "%s".

Parameters

serverAddress (STRING): Address of the LDAP server that is not responding fast enough.
vserverName (STRING): SVM associated with this operation.

secd.lsa events

secd.lsa.noServers

Severity

EMERGENCY

Description

This message occurs when none of the configured LSA servers are accepting connections.

Corrective Action

Ensure that all configured LSA servers are responding to requests. Ensure that there are no networking issues stopping the cluster from communicating with the configured LSA servers.

Syslog Message

None of the LSA servers configured for Vserver (%s) are currently accessible via the network.

Parameters

vserverName (STRING): vserver associated with this operation.

secd.nametrans events

secd.nameTrans.groupNotFound

Severity

ERROR

Description

This message occurs when the group name cannot be resolved by any of the entities in the ns-switch for the virtual server.

Corrective Action

If this is a Windows® name, make sure that the name exists in Active Directory. If this is a UNIX® name, make sure that it is in one of the configured ns-switch entities for the virtual server. Make sure that it was entered locally as a unix-group, in the Network Information Service (NIS) maps, or in the Lightweight Directory Access Protocol (LDAP) server.

Syslog Message

vserver (%s) could not resolve the group name (%s) by any of the entities in the ns-switch for the virtual server.

Parameters

vserverName (STRING): vserver associated with this operation.
groupName (STRING): Name of the group that could not be converted to an ID.

secd.nameTrans.invalidConfig

Severity

ERROR

Description

This message occurs when the name resolution configuration for the virtual server is not set up correctly.

Corrective Action

Consult the documentation and correct the ns-switch entry for the virtual server.

Syslog Message

vserver (%s) has an incorrectly configured ns-switch. Check all of the virtual servers to ensure that the ns-switch has been configured correctly.

Parameters

vserverName (STRING): vserver associated with this operation.

secd.nameTrans.invalidUser

Severity

ERROR

Description

This message occurs when the user name cannot be resolved by any of the entities in the ns-switch for the virtual server.

Corrective Action

If this is a Windows® name, make sure the name exists in Active Directory. If this is a UNIX® name, make sure it is in one of the configured ns-switch entities for the virtual server. Make sure that the name was entered locally as a unix-user, in the Network Infomration Service (NIS) maps, or in the Lightweight Directory Access Protocol (LDAP) server.

Syslog Message

vserver (%s) could not resovle user name (%s).

Parameters

vserverName (STRING): vserver associated with this operation.
userName (STRING): Name of the user that could not be converted to an ID.

secd.nameTrans.noNameMapping

Severity

ERROR

Description

This message occurs when no name mappings or default-users are defined to convert a Windows® name to a UNIX® name or a UNIX name to a Windows name.

Corrective Action

Make sure that a default Windows user is defined for the Network File System (NFS) configuration. Make sure that a default UNIX user is defined for the CIFS configuration. Decide to either to create one of the

previously mentioned items, or create a mapping rule that maps the user or group in the correct direction.

Syslog Message

vserver (%s) could not map name (%s). Reason: %s.

Parameters

vserverName (STRING): vserver associated with this operation.
userName (STRING): Name of the user that could not be converted to an ID.
attemptedMapping (STRING): Description of the specific error condition.

secd.nameTrans.unknownUser

Severity

ERROR

Description

This message occurs when the user name cannot be resolved by any of the entities in the ns-switch for the virtual server.

Corrective Action

If this is a Windows® name, make sure that the name exists in Active Directory. If this is a UNIX® name, make sure that it is in one of the configured ns-switch entities for the virtual server. Make sure that it was entered locally as a unix-user, in the Network Information Service (NIS) maps, or in the Lightweight Directory Access Protocool (LDAP) server.

Syslog Message

vserver (%s) could not resolve the user name (%s) by any of the entities in the ns-switch for the virtual server

Parameters

vserverName (STRING): vserver associated with this operation.
userName (STRING): Name of the user that could not be converted to an ID.

secd.nameTrans.userNotFound

Severity

ERROR

Description

This message occurs when the user name cannot be resolved by any of the entities in the ns-switch for the virtual server.

Corrective Action

If this is a Windows® name, make sure that the name exists in Active Directory. If this is a UNIX® name, make sure it is in one of the configured ns-switch entities for the virtual server. Make sure that it was entered locally as a unix-user, in the Network Information Service (NIS) maps, or in the Lightweight Directory Access Protocol (LDAP) server.

Syslog Message

vserver (%s) could not resolve the user name (%s) by any of the entities in the ns-switch for the virtual server.

Parameters

vserverName (STRING): vserver associated with this operation.
userName (STRING): Name of the user that could not be converted to an ID.

secd.netgroup events

secd.netgroup.ldap.badFilter

Severity

ERROR

Description

This message occurs if the filter for searching the Lightweight Directory Access Protocol (LDAP) server is found to be invalid. The typical reason for this issue is incorrect LDAP client configuration or a bad netgroup name. Searching for the current netgroup is skipped, so all hosts in the netgroup might not be authorized.

Corrective Action

Use the "vserver services name-service ldap client schema show" command to ensure that the Object Class and Attribute in the LDAP client schema are correct. Check the LDAP configuration on the server side to ensure that the attribute value (such as nisNetgroup) is correct.

Syslog Message

LDAP search on vserver (%s) failed on invalid filter: %s.

Parameters

vserverName (STRING): The name of the Vserver associated with this operation.
filter (STRING): The invalid filter that caused the LDAP search to fail.

secd.netlogon events

secd.netlogon.noServers

Severity

EMERGENCY

Description

This message occurs when none of the configured Netlogon servers are accepting connections.

Corrective Action

Ensure that all configured Netlogon servers are responding to requests. Ensure that there are no networking issues stopping the cluster from communicating with the configured Netlogon servers.

Syslog Message

None of the Netlogon servers configured for Vserver (%s) are currently accessible via the network.

Parameters

vserverName (STRING): vserver associated with this operation.

secd.nfs events

secd.nfs.groupLimit

Severity

ERROR

Description

This message occurs when Data ONTAP® truncates the number of groups to which a user belongs. This can happen when a user of a UNIX-based system is in more groups than the limit supported by the system.

Corrective Action

Determine the maximum number of groups allowed for the Vserver in question with the "nfs show -vserver <vservername> -fields extended-groups-limit" command. If necessary, configure the limit of extended groups on the Vserver by using the (privilege mode: advanced) command "nfs modify -vserver <vsname> -extended-groups-limit <0..1024>". Make sure that the user does not belong to more than the maximum number of groups supported on the site NIS or LDAP server. (This maximum should correspond to the value of the "extended-groups-limit" field that was either displayed or set in the given commands.)

Syslog Message

User (%s) is in too many groups (%d): on Vserver (%s).

Parameters

uname (STRING): UNIX user name.
gidCount (INT): Total number of auxillary groups that a user belongs to, in various name services.
vserverName (STRING): Name of the Vserver.

secd.nfsauth events

secd.nfsAuth.noCifsCred

Severity

ERROR

Description

This message occurs when an NFS authorization attempt fails because of the inability of the system to retrieve a matching CIFS credential for use in multi-protocol security operations.

Corrective Action

Examine the failure details to determine corrective action. This failure usually occurs because the system is unable to communicate with Active Directory.

Syslog Message

vserver (%s) NFS authorization cannot retrieve CIFS credentials. %s

Parameters

vserverName (STRING): vserver associated with this operation.
failureDetail (STRING): Error journal is a collection of events leading up to a failure. This failure is likely to impact many (if not all) users, and might reflect a misconfiguration or environmental problem..

secd.nfsAuth.noCifsSid

Severity

ERROR

Description

This message occurs when an NFS authorization attempt fails because the system could not resolve an associated Windows security identifier (SID).

Corrective Action

Examine the failure details to determine corrective action. This failure usually occurs because the system is unable to communicate with Active Directory.

Syslog Message

vserver (%s) Unable to resolve CIFS security identifier (SID). %s

Parameters

vserverName (STRING): vserver associated with this operation.
failureDetail (STRING): Error journal is a collection of events leading up to a failure. This failure is likely to impact many (if not all) users, and might reflect a misconfiguration or environmental problem..

secd.nfsAuth.noCifsUser

Severity

ERROR

Description

This message occurs when an NFS authorization attempt fails because the Windows user that NFS maps to cannot be found.

Corrective Action

Examine the failure details to determine corrective action. Common failures include faulty UNIX-to-Windows name mapping rules, an improperly configured default Windows user, or the system is unable to communicate with Active Directory.

Syslog Message

vserver (%s) Mapped CIFS user name not found. %s

Parameters

vserverName (STRING): vserver associated with this operation.
failureDetail (STRING): Error journal is a collection of events leading up to a failure. This failure is likely to impact many (if not all) users, and might reflect a misconfiguration or environmental problem..

secd.nfsAuth.noNameMap

Severity

ERROR

Description

This message occurs when an NFS authorization attempt fails because of a UNIX to Windows name mapping issue.

Corrective Action

Examine the failure details to determine corrective action. Common failures include no appropriate UNIX-to-Windows name mapping rules, no configured default Windows user, or the inability of the system to contact LDAP if LDAP is configured for name mapping.

Syslog Message

vserver (%s) Cannot map UNIX name to CIFS name. %s

Parameters

vserverName (STRING): vserver associated with this operation.
failureDetail (STRING): Error journal is a collection of events leading up to a failure. This failure is likely to impact many (if not all) users, and might reflect a misconfiguration or environmental problem..

secd.nfsAuth.noUnixCreds

Severity

ERROR

Description

This message occurs when an NFS authorization attempt fails because credentials for a UNIX user cannot be determined.

Corrective Action

Examine the error journal for the collection of events that led to the specific failure. A common failure is the inability to communicate with NS-SWITCH authorization sources.

Syslog Message

Vserver "%s" cannot determine UNIX identity. %s

Parameters

vserverName (STRING): Vserver associated with this operation.
failureDetail (STRING): Error journal is a collection of events leading up to a failure. This failure is likely to impact many (if not all) users, and might reflect a misconfiguration or environmental problem.

secd.nfsAuth.problem

Severity

ERROR

Description

This message occurs when an NFS authorization attempt fails.

Corrective Action

Examine the failure details to determine corrective action. Common failures include name mapping issues, or the inability to communicate with domain controllers, NIS servers, or LDAP servers due to connectivity or configuration problems.

Syslog Message

vserver (%s) General NFS authorization problem. %s

Parameters

vserverName (STRING): vserver associated with this operation.
failureDetail (STRING): Error journal is a collection of events leading up to a failure. This failure is likely to impact many (if not all) users, and might reflect a misconfiguration or environmental problem..

secd.nis events

secd.nis.connectFailure

Deprecated

Deprecated as of version 9.5 since this EMS is no longer needed.

Severity

ALERT

Description

This message occurs when the server could not establish a TCP connection to a Network Information Service (NIS) server.

Corrective Action

From a UNIX ® workstation, make sure that the NIS server is responding to requests. Also make sure that the portmapper on the NIS server is responding to requests. Make sure that there are no networking issues stopping the cluster from communicating with this NIS server.

Syslog Message

vserver (%s) could not make a connection over the network to NIS server (%s) at address (%s) and received error (%s)

Parameters

vserverName (STRING): vserver associated with this operation.
serverName (STRING): Name of the NIS server that was not responding.
serverAddress (STRING): Address of the NIS server that was not responding.
ErrnoMessage (STRING): Errno message from the connect failure.

secd.nis.noServers

Deprecated

Deprecated as of version 9.5 since this EMS is no longer needed.

Severity

EMERGENCY

Description

This message occurs when none of the configured Network Information Service (NIS) servers are accepting connections.

Corrective Action

From a UNIX® workstation, make sure that all configured NIS servers are responding to requests. Ensure that there are no networking issues stopping the cluster from communicating with the configured NIS servers. Also, ensure that the portmapper running on the NIS server is working correctly.

Syslog Message

None of the NIS servers configured for Vserver (%s) are currently accessible via the network.

Parameters

vserverName (STRING): vserver associated with this operation.

secd.nis.slowServer

Deprecated

Deprecated as of version 9.5 since this EMS is no longer needed.

Severity

ERROR

Description

This message indicates that the Network Information Service (NIS) server is not responding to requests in the expected time frame.

Corrective Action

Make sure that there are no networking issues creating intermittent communication problems with the NIS server. Make sure that the machine running NIS is responsive and not overloaded. From a UNIX ® workstation, run YP commands to verify long response times.

Syslog Message

From CIFS Server(%s) calls to NIS server (%s) at address (%s) is executing slowly enough to adversely impact the performance of your server.

Parameters

vserverName (STRING): vserver associated with this operation.
serverName (STRING): Name of the NIS server that was not responding fast enough.
serverAddress (STRING): Address of the NIS server that was not responding fast enough.

secd.nonetgroupfile events

secd.noNetgroupFile

Severity

ALERT

Description

This message occurs when trying to process a netgroup in an export policy while the Vserver "ns-switch" option is set exclusively to "file" but no netgroup file is loaded. Client requests cannot be processed until a netgroup file is loaded or another name service is added to the Vserver "ns-switch" option.

Corrective Action

Load a netgroup file for the Vserver by using the "netgroup load" command, or add another name service to the Vserver "ns-switch" option.

Syslog Message

Cannot evaluate a netgroup in an export policy without a properly configured "ns-switch" option for Vserver "%s". It is set exclusively to "file" but no netgroup file is loaded.

Parameters

vserverName (STRING): Vserver associated with this operation.

secd.quark events

secd.quark.ddns.updt.failure

Severity

ERROR

Description

This message occurs when the server can not a send dynamic DNS (DDNS) update to the DNS server.

Corrective Action

For "NOTIMP" errors, enable DDNS on the DNS server. For "REFUSED" errors, verify the DDNS settings on the DNS server. For all other errors, Contact NetApp technical support..

Syslog Message

DDNS update failed with error %s.

Parameters

cmdError (STRING): Error from the attempted DDNS update.

secd.quark.sid.lookup.failed

Severity

ERROR

Description

This message occurs when the Active Directory server cannot find the Security Identifier (SID) for a given account name.

Corrective Action

Provide a valid account name.

Syslog Message

Failed to lookup the SID for account name "%s" with error "%s".

Parameters

accountName (STRING): Name of the account whose SID is looked up in the server.
errorMsg (STRING): Error received from the server while doing a SID lookup for the given account name.

secd.rpc events

secd.rpc.authRequest.blocked

Severity

ALERT

Description

This message occurs when a CIFS authentication RPC is blocked by Security Daemon(SecD) due to continuous authentication requests with wrong logon password from a particular client.

Corrective Action

Check whether there is an unexpected increase in the number of authentication requests with wrong logon password from a particular CIFS client.

Syslog Message

Too many CIFS authentication attempts with wrong password from client "%s" on Vserver "%s".

Parameters

clientIP (STRING): Client that has been blocked.
vserverName (STRING): Vserver associated with this operation.

secd.rpc.server.ready

Severity

INFORMATIONAL

Description

This message occurs when SecD successfully loads the configuration and is ready to serve all RPCs.

Corrective Action

(None).

Syslog Message

SecD is ready to serve all RPCs.

Parameters

(None).

secd.rpc.server.request.dropped

Severity

ERROR

Description

This message occurs when a remote procedure call(RPC) is dropped by SecD due to a lack of memory space. It might occur either when SecD receives too many requests than it can handle or when a number of requests have accumulated due to server connectivity issues.

Corrective Action

Check whether there is an unexpected increase in the number of authentication requests from NFS/CIFS clients. Verify that there are no connectivity issues to the external servers like DNS, LDAP, and DC.

Syslog Message

RPC "%s" that was sent from "%s" was dropped by SecD due to a lack of memory space.

Parameters

rpcName (STRING): Name of the RPC that has been dropped.

callerName (STRING): Caller of the RPC that has been dropped.

secd.single events

secd.single.label.domain

Severity

ERROR

Description

This message occurs when the trusted domains for the CIFS home domain of a Vserver contains a single-label domain (SLD). An SLD configuration is not supported because it can cause CIFS access issues.

Corrective Action

Examine and remove any SLDs configured for the CIFS domain associated with the corresponding Vserver on your domain controller. Additionally, examine and revoke any account's access to the CIFS server where the account is from the trusted SLD.

Syslog Message

Single-label domain (SLD) "%s" was found in the CIFS trusted domains for Vserver %s.

Parameters

domainName (STRING): Trusted SLD.
vserverName (STRING): Vserver associated with this operation.

secd.strong events

secd.strong.auth.required

Severity

ALERT

Description

This message occurs when the external LDAP server configured for a Vserver is enforcing stronger authentication than what the ONTAP® LDAP client is configured for.

Corrective Action

Configure stronger LDAP session security using the following commands: 1. vserver services name-service ldap client modify -session-security 2. vserver cifs security modify -session-security-for-ad-ldap

Syslog Message

Stronger authentication enforced by LDAP server for Vserver %s.

Parameters

vserverName (STRING): Vserver associated with this operation.

secd.unexpectedfailure events

secd.unexpectedFailure

Severity

ERROR

Description

This message occurs when the security daemon captures an unexpected failure.

Corrective Action

Examine the failure details to determine corrective action.

Syslog Message

Unexpected SecD failure in Vserver "%s". Details: %s

Parameters

vserverName (STRING): Vserver associated with this operation.
failureDetail (STRING): The error journal documents the events leading up to the failure. This failure is likely to impact many (if not all) users, and it might indicate a misconfiguration or environmental problem.

secd.unixlookupfailure events

secd.unixLookupFailure

Severity

ERROR

Description

This message occurs when an UNIXi® user or group lookup fails. This failure is likely to impact many or all users, and might indicate a misconfiguration or environmental problem.

Corrective Action

Examine the error journal in the /mroot/etc/mlog/secd.log file to learn more about why the LOOKUP failed. The error journal is a collection of events leading up to a failure. Common failures include the wrong user name or ID and the inability to communicate with the NIS or LDAP servers due to connectivity or configuration problems. If the vserver's NSSWITCH is set to "file", verify that the user or group that is being looked up has been created using the cluster's ngshell interface. If the vserver's NSSWITCH is set to "NIS", run 'yp' commands from an NIS client workstation to verify that the UNIX lookup works on the configured NIS server. If the vserver's NSSWITCH is set to "LDAP", run 'ldap' commands from an LDAP client workstation to verify that the UNIX lookup works on the configured LDAP server. Verify that the cluster can communicate with the configured NIS or LDAP servers.

Syslog Message

UNIX lookup failure on Vserver (%s) for client with IP address (%s). %s

Parameters

vserverName (STRING): vserver associated with this operation.
clientIP (STRING): IP Address of the client.
failureDetail (STRING): Reason for the failure.

Copyright information

Trademark information