ARX SNMP Reference

810-0041-00

Publication Date

This manual was published on June 1, 2012.

Legal Notices

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

3DNS, Access Policy Manager, Acopia, Acopia Networks, Advanced Client Authentication, Advanced Routing, APM, Application Security Manager, ARX, AskF5, ASM, BIG-IP, Cloud Extender, CloudFucious, CMP, Data Manager, DevCentral, DevCentral [DESIGN], DNS Express, DSC, DSI, Edge Client, Edge Gateway, Edge Portal, EM, Enterprise Manager, F5, F5 [DESIGN], F5 Management Pack, F5 Networks, F5 World, Fast Application Proxy, Fast Cache, FirePass, Global Traffic Manager, GTM, IBR, Intelligent Browser Referencing, Intelligent Compression, IPv6 Gateway, iApps, iControl, iHealth, iQuery, iRules, iRules OnDemand, iSession, IT agility. Your way., L7 Rate Shaping, LC, Link Controller, Local Traffic Manager, LTM, Message Security Module, MSM, Netcelera, OneConnect, Packet Velocity, Protocol Security Module, PSM, Real Traffic Policy Builder, ScaleN, SSL Acceleration, StrongBox, SuperVIP, SYN Check, TCP Express, TDR, TMOS, Traffic Management Operating System, TrafficShield, Transparent Data Reduction, VIPRION, vCMP, WA, WAN Optimization Manager, WANJet, WebAccelerator, WOM, and ZoneRunner, are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by U.S. Patents 7,877,511; 7,958,347. This list is believed to be current as of June 1, 2012.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

This product includes software from several third-party vendors. Each vendor is listed below with the applicable copyright.

Unless otherwise noted, the companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Revision History

October 2005 - Rev A

March 2006 - Rev B, Software Release 2.1.4

April 2006 - Rev C, Software Release 2.3

July 2006 - Rev D, updates for Software Release 2.4

October 2006 - Rev E, add dynamic-DNS traps for Software Release 2.4.2

January 2007 - Rev F, updates for Software Release 2.4.3

March 2007 - Rev G, updates for Software Release 2.5.0

May 2007 - Rev H, updates for Software Release 2.5.1

August 2007 - Rev J, new CPU trap for Software Release 2.6.0

December 2007 - Rev K, several new traps for Software Release 3.0.0

March 2008 - Rev L, several new traps for Software Release 3.1.0; convert to F5 format

June 2008 - Rev M, updates for Software Release 4.0.0

October 2008 - Rev N, re-brand the OS

June 2009 - Rev P, several new traps for Software Release 5.00.000

November 2009 - Rev Q, new traps for Software Release 5.01.000

October 2010 - Rev R, new traps for Software Release 5.02.000

January 2011 - Rev S, minor changes for Software Release 5.03.000

June 2011 - Rev T, new traps for Software Release 6.00.000

September 2011 - Rev U, new traps for Software Release 6.01.000

July 2012 - Rev V, new traps for Software Release 6.02.000

1

SNMP Reference

This manual lists the SNMP MIBs and describes the SNMP traps supported by the ARX®. Use this as a companion document with the *ARX® CLI Reference*.

The ARX supports SNMPv2c data collection.

Supported MIBs

Different ARX platforms have different SNMP MIBs, tailored to support the hardware and/or software configuration of each platform.

The ARX-1500 and ARX-2500 support the following MIBs:

- RFC 1213 - MIB-II - mib-2.my

  This includes the sysORTable(.1.9), which lists supported MIBs.
- If (interface) MIB - ifmib.my
- IfType MIB - ifType.my
- SNMPv2 MIB - snmpv2-mib.my
- Dot1q MIB - vlan.my
- Dot3ad MIB - dot3ad.my
- RFC 2737 - Entity MIB - entity.my
- F5 Data Solutions's Enterprise MIB, acopiasmi.my. The traps for this MIB are described in this manual. You can use a standard MIB browser to view documentation for all of the remaining OIDs.

The ARX-VE supports a smaller set of MIBs:

- RFC 1213 - MIB-II - mib-2.my

  This includes the sysORTable(.1.9), which lists supported MIBs.
- If (interface) MIB - ifmib.my
- IfType MIB - ifType.my
- SNMPv2 MIB - snmpv2-mib.my
- Dot1q MIB - vlan.my
- F5 Data Solutions's Enterprise MIB, acopiasmi.my.

All other ARX devices support the following, larger, set of MIBs:

- RFC 1213 - MIB-II - mib-2.my

  This includes the sysORTable(.1.9), which lists supported MIBs.
- If (interface) MIB - ifmib.my
- IfType MIB - ifType.my
- SNMPv2 MIB - snmpv2-mib.my
- Dot1q MIB - vlan.my
- Dot3ad MIB - dot3ad.my
- PBridge MIB - pbridge.my
- RFC 2668 - IEEE 802.3 MIB - rfc2668.my
- RFC 1493 - Bridge MIB - bridge.my
- RFC 1643 - Etherlike MIB - etherlike.my
- RFC 2674 - Bridges with Traff MIB
- RFC 2737 - Entity MIB - entity.my

- RFC 2819 - RMON MIB, groups 1, 2, 3, and 9 - rmon.my
- F5 Data Solutions's Enterprise MIB, acopiasmi.my. The traps for this MIB are described in this manual. You can use a standard MIB browser to view documentation for all of the remaining OIDs.

Use the show software command for a complete list of these MIBs; these are the files with ".my" extensions. A zipped tar file, "Mibs.tgz," includes all of these MIBs and an "openview.trapd.conf" file to be used with HP OpenView. Use copy ftp, copy scp, or copy tftp to upload "Mibs.tgz" to a management station with a MIB browser. You can unzip and untar the file at the management station to get all of the individual MIB files and openview.trapd.conf.

The openview.trapd.conf file is a text file with instructions at the top. If your management station supports HP OpenView, you can use these instructions to merge the file with your current trapd.conf file. After this merge, ARX traps are available in the OpenView Events browser.

Generic Traps

The ARX supports the generic traps defined in RFC 1157, the specification for SNMP:

- coldStart
- warmStart

  This indicates that the ARX rebooted. If planned, this was initiated by the reload command or its GUI equivalent. An unplanned reboot emits an autoReboot trap, too. This trap can be configured as an email event (see email-event). It is part of the "chassis" event group.
- linkDown
- linkUp
- authenticationFailure
- entityConfigChange (defined in the RFC as an enterpriseSpecific trap)

Enterprise Traps

This section explains all of the ARX-Enterprise traps. Each trap name appears in bold text, followed by the last component in its OID (1.3.6.1.4.1.13544.2.1.0.*nnn*). The description explains how to react to or recover from each event, with links to detailed command explanations in the *ARX® CLI Reference*.

ARX Reboots

autoReboot (10) - The redundancy software detected a failure and triggered a reboot on this switch. This causes a failover to the other peer.

For a planned reboot (initiated by the reload command or its GUI equivalent), the ARX sends a warmStart trap, described above.

bounceLimitRaise (15) - The ARX has rebooted three times in less than 24 hours due to software faults. This trap indicates that the ARX has suspended all reboots caused by software faults (though other conditions, such as a catastrophic hardware failure, may still trigger a reboot). Use the collect diags command to collect diagnostic information and send it to F5 Support. After the software problem is diagnosed and resolved, a manual reload clears this alarm condition.

You can configure this trap as an email event (see email-event). It is part of the “chassis” event group.

bounceLimitClear (16) - reserved for internal use only.

Active-Directory (AD)

adDiscoveryStart (11) - The ARX began an auto-discovery operation to find the Domain Controllers (DCs) in an Active-Directory (AD) forest. A CIFS front-end service uses this information to facilitate Kerberos authentication for its clients. This trap indicates that an administrator or script invoked the active-directory update seed-domain command, the active-directory update forest command, or their GUI equivalents.

adDiscoveryComplete (13) - The ARX has successfully discovered the DCs in an AD forest, and has updated the AD-forest configuration in its database. A CIFS service can now use Kerberos to authenticate all of the forest’s CIFS clients. The discoveries are listed in the AD-discovery report, named “active-directory-*forest_name*.rpt.” The *forest_name* is identified in the trap text. Use show reports report-name to find and view the AD-discovery report.

adDiscoveryFail (12) - An AD-discovery operation has failed. The trap text briefly describes the failure. The configuration information about the AD forest has not been changed in the ARX database. The details of the failure appear in the AD-discovery report, named “active-directory-*forest_name*.rpt.” The *forest_name* is identified in the trap text. Use show reports report-name to find and view the AD-discovery report.

adPolicyViolationRaise (31) - An external AD policy or constraint has caused the active-directory alias command to fail for an ARX service. This command sets a Service-Principal Name (*SPN*) for the ARX service; the DC disallowed the operation, perhaps because the service has reached the maximum number of SPNs allowed. To clear this alarm condition, remove the constraint from the AD database . The Windows domain and the ARX service’s FQDN are included in the trap. You can use the show active-directory status command to find the active DCs that the ARX uses for the Windows domain.

This trap is always accompanied by a ’spnAliasUpdateRaise’ trap. This trap indicates the specific cause of the spnAliasUpdateRaise trap. Together, they indicate a single issue.

You can configure this trap as an email event (see email-event). It is part of the “network” event group.

adPolicyViolationClear (32) - The active-directory alias operation succeeded for the first time since the ’adPolicyViolationRaise’ condition went into effect. The ARX service is no longer bound by the external constraint.

This trap is always accompanied by a ’spnAliasUpdateClear’ trap. Together, they indicate that a single issue is now cleared.

Archive Share for File Tracking

Each of these traps can be configured as an email event (see email-event), except as otherwise noted. They are part of the “storage” event group.

archiveOffline (14) - The ARX lost contact with a filer share that is being used as a file-history archive. The filer IP and share name are included in the trap text. One or more managed volumes use this share to store their file-history records, so that users can query for the back-end location of a file at any given time. Check the connection to the filer and correct the problem as soon as possible. You can use the ping and expect traceroute commands to verify connectivity from the ARX. You can also use show exports to check the state of the NFS and/or CIFS service at the filer.

archiveOnline (17) - An administrator has added a new file-history archive, or an existing file-history archive has recovered from the ‘archiveOffline’ state.

archiveFreeSpaceThresholdRaise (19) - The external-filer share (or managed volume) behind a file-history archive has less than 10 G (Gigabytes) of free space. The share name are included in the trap. You can use the show file-history archive ... contents command to see the records on the share, and you can use clear file-history archive to clear some of them. Alternatively, you can use the location command to change the location of the archive.

If the archive resides on a managed volume, you also have the option to add more filer shares behind the volume (with share and its sub commands) to increase your storage space.

archiveFreeSpaceThresholdClear (18) - A formerly-full archive now has enough free space, 10.5 G (Gigabytes), to clear the “full” condition. This indicates that the file-history archive has recovered from the ’archiveFreeSpaceThresholdRaise’ state.

archiveRemove (21) - An administrator removed a file-history archive from the ARX configuration. This is the result of a no file-history archive or no location command, or their GUI equivalents. The removed archive is identified in the trap by its filer IP and its share name at the filer.

archiveWriteAccessFail (22) - The ARX tried and failed to write to a file-history archive’s location. The location is on either an external-filer share or a managed volume. The trap shows the intended destination, including the name of the share. You can use show file-history archive *archive-name* to find the exact location (including the directory path) for a given archive; check the location to confirm that the share and path still exist.

This trap may also indicate a problem with write permission at the location. If this is a CIFS share, the location’s assigned proxy-user has the permission issue. Use show file-history archive *archive-name* to find the proxy user that you are using for this archive, and run the location command if you want to select a new proxy user. If the location is on a managed volume, this could indicate a permission problem with the proxy-user (gbl-ns) assigned to the volume’s namespace, and it indicates a larger problem with the volume itself.

If the location is on an NFS export, the ARX runs its write test as *root*. Check the filer itself and ensure that root squashing is disabled for the chosen export. As above, this indicates a larger problem if the location is on a managed volume.

For a location on an external filer, you can use show exports to confirm that *root* or a particular proxy user have write permission at the share or export.

archiveWriteAccessClear (23) - An archive that formerly blocked write access is now allowing writes. This indicates that the file-history archive has recovered from the ’archiveWriteAccessFail’ state.

archiveWriteProbeFail (24) - The ARX tried and failed to write a test file on the location share for a file-history archive. This is not a permission failure, it is an indication that the test stopped before it was complete. If the location is on an external filer, you can use the ping and expect traceroute commands to check connectivity to the back-end filer. If the location is on a managed volume, there may be a problem connecting to the filer shares behind it.

Unlike the traps above, this cannot be configured as an email Event.

Auto Diagnostics

These traps are from the auto-diagnostics subsystem, which periodically collects statistical data and sends it to one or more email recipients. These email recipients (including F5) can monitor this data over time and take preventative action if there are any undesirable trends.

Each of these traps can be configured as an email event (see email-event), except as otherwise noted. They are part of the “chassis” event group.

autoDiagnosticsFailedRaise (25) - The auto-diagnostics subsystem has failed to deliver diagnostics to its email recipients. The failure may have occurred during information collection or email delivery; see the error message in the trap for further details. You can use the show auto-diagnostics command for the configuration and state of the auto-diagnostics subsystem, and you can use show smtp status for the configuration and state of the SMTP (email) software.

autoDiagnosticsFailedClear (26) - The auto-diagnostics subsystem successfully delivered diagnostics to its email recipients after a previous failure. This indicates that the auto-diagnostics subsystem has recovered from the ’autoDiagnosticsFailedRaise’ state.

The ARX also sends this trap if someone uses the no auto-diagnostics command to shut down auto-diagnostics processing.

Broadcast Storm

broadcastStormRecoveryStart (20) - reserved for future use.

broadcastStormRecoveryEnd (30) - reserved for future use.

Clock

clockChange (37) - Either an administrator used the clock set (or clock timezone) command to change the ARX’s time, or the NTP server caused a time change. A large time change can cause problems for policy, Kerberos authentication, and RON communication.

Use the show ntp servers command to show the NTP server(s) for the switch.

Config-Replication (to Prepare for Disaster Recovery)

Each of these traps can be configured as an email event (see email-event), except as otherwise noted. They are part of the “network” event group.

configReplicationFailRaise (38) - A config-replication rule failed in an attempt to copy the global configuration from one ARX cluster to another. The name of the destination ARX (which did not receive the copy) is included in the trap. For details, refer to the report produced by the config-replication rule. You can also use the show ron command to verify that the connection between the source and destination ARX (a RON tunnel) is functional. You should resolve this issue to ensure that the backup cluster has the latest global configuration, in case the active cluster experiences an unexpected outage.

configReplicationFailClear (39) - A config-replication rule succeeded in copying a global-config file to the backup cluster. This occurred after a previous failure. This trap announces that the ARX has recovered from the ’configReplicationFailRaise’ condition.

Core Files

coreFile (40) - A system failure occurred, and the system is generating a core-memory file for diagnosis.

coreFileDelete (50) - An old core file was deleted to make room for a new one.

coreFileDeleteDuplicate (60) - The core-harvester process found a duplicate core file and deleted it to conserve disk space.

CPUs

cpuHalt (68) - A CPU has stopped processing. The ARX has several failure-recovery mechanisms that may return the CPU to service. This trap can result from a firmware upgrade, which halts all CPUs and reboots them; check for a ’firmwareUpgradeInitiated’ trap that may have preceded this one.

In any case, allow a minute or two for recovery. A recovery is announced by a cpuStatus trap (see below) that indicates a positive change in status.

If the system does not send a positive cpuStatus trap, contact F5 Support for guidance.

This trap can be configured as an email event (see email-event). It is part of the “chassis” event group.

cpuFail (69) - An NSM-core processor could not go into “standby” state after its host processor failed over. This is one NSM core on a physical NSM processor, where the physical NSM processor failed over to a peer processor.

The ARX does not have nsm recovery enabled (some ARX platforms cannot support that feature), so the NSM core in the trap is not in “standby” state. If there is a later NSM-core fail back, the core cannot take over network processing.

Contact F5 Support if you see this trap.

cpuStatus (70) - A CPU has changed from a failure state to a running state. (The trap specifies the slot number and processor number.) The CPU states are the same as the operational states shown by the show processors command.

cpuTempFail (73) - A CPU's temperature is too high. The trap specifies the slot number and processor number for this CPU. You can use the show chassis temperature command to find the current temperature of the CPU.

This trap can be configured as an email event (see email-event). It is part of the "chassis" event group.

cpuTempStatus (74) - A CPU's temperature that was formerly too high has cooled to an acceptable temperature range. As above, the trap specifies the CPU's slot number and processor number. This clears the alarm status that is raised by the cpuTempFail trap.

This trap can be configured as an email event (see email-event). It is part of the "chassis" event group.

Critical Resources (Redundancy)

criticalResourceAllHealthy (80) - All critical resources (such as a critical route or a critical namespace share) on the trapping host are now online; the redundant peer can now fail over to this peer for critical-resource related reasons. The associated message is "All critical services are ONLINE."

criticalResourceDeConfig (90) - An administrator has removed a (former) critical resource from the list of critical resources.

criticalResourceFailureReboot (100) - A critical resource has failed and the peer switch can accept a failover, so the trapping switch is rebooting and failing over.

criticalResourceOffline (110) - A critical resource has failed. The name of the critical resource is included in the trap.

criticalResourceOnline (120) - An administrator has added a new critical resource, or an existing critical resource has recovered from the 'criticalResourceOffline' state. The name of the critical resource is included in the trap.

Database Upgrade Failures

Each of these traps can be configured as an email event (see email-event). They are part of the "chassis" event group.

dbUpgradeFailRaise (125) - A software upgrade failed to update the configuration database. The overall software upgrade cannot continue. Use the boot system command to select the previously-running release, then use reload to put the previous release back in service. Use the run configs *running-config* command to restore your previous running-config. If this ARX is a standalone switch (that is, not part of a redundant pair), you must also use run configs *global-config* to restore the global-config.

Contact F5 Support if you receive this trap.

dbUpgradeFailClear (126) - Is used for internal testing only. The alarm condition from ’dbUpgradeFailRaise’ is cleared when you reload the ARX to downgrade the software, as described above.

Directory-Attribute Inconsistencies

A managed volume keeps multiple copies of its directories on multiple back-end shares, and always attempts to keep the attributes of those directories consistent. (Directory attributes are the user ID for the directory owner, one or more ACLs for the directory, and similar data.) There are some situations where it is impossible to keep the attributes consistent, such as when one of the back-end shares runs out of disk space and cannot store a new set of ACLs. These traps relate to such failures.

Each of these traps can be configured as an email event (see email-event). They are part of the “storage” event group.

directoryAttributeInconsistencyRaise (152) - A managed-volume directory has attributes that are inconsistent between back-end shares. The directory is included in the trap text, as well as the IP address of the back-end filer that refused the command to set attributes. You can access this filer directly to address the issue, perhaps by adding more disk space or raising a quota. If the issue is free space, you can also create a place-rule to migrate files from the full share to one with more space. As a final alternative, you can access the VIP as a client and remove files from that directory; the find command shows the back-end location of any given file.

directoryAttributeInconsistencyClear (153) - A directory with formerly-inconsistent attributes is now consistent. Someone has cleared the error condition (typically a disk-space issue) at one of the directory’s backing filers, shown in the trap. This clears the alarm condition raised by the directoryAttributeInconsistencyRaise trap.

directoryAttributeInconsistencyClearAll (154) - An entire share has had all of its directory-inconsistency alarms cleared at once. This is typically caused by the share being removed from the volume, through remove-share migrate, remove-share nomigrate, nsck ... rebuild, nsck ... destage, or a similar command.

directoryImportStalledRaise (155) - A managed-volume has stalled its import of a back-end share because it is unable to set attributes on one of its directories. The directory is included in the trap text, as well as the IP address of the back-end filer that refused the command to set attributes. You can access this filer directly to address the issue, perhaps by adding more disk space or raising a quota.

directoryImportStalledClear (156) - A share whose import was stalled due to inconsistent-directory attributes is now importing. Someone has cleared the error condition (typically a disk-space issue) at one of the directory's backing filers, shown in the trap. This clears the alarm condition raised by the directoryImportStalledRaise trap.

directoryImportStalledClearAll (157) - An entire share has had all of its stalled-import alarms cleared at once. This is typically caused by the share being removed from the volume, through remove-share migrate, remove-share nomigrate, nsck ... rebuild, nsck ... destage, or a similar command.

Disks (Internal to the ARX)

These traps apply to the disks that are internal to the ARX chassis. The disks store configuration files, log files, and other information that is useful to the CLI or ARX Manager (GUI).

Each of these traps can be configured as an email event (see email-event). They are part of the "chassis" event group.

diskCtlFail (129) - The drive controller detected a marginal disk drive; the current transfer rate is less than the maximum. (You can use show chassis diskuse to view the maximum rate.) This trap indicates that the drive is not running at optimum speed, and may fail soon. You can use raid rebuild to try to rebuild the disk. If this fails, contact F5 Support to get a replacement drive.

diskCtlStatus (130) - The drive controller changed a disk drive's status from "Failed" to another state.

diskFail (131) - A removable disk failed. Use raid rebuild to rebuild the disk. If this fails, contact F5 Support to get a replacement.

diskStatus (132) - A removable disk changed to an non-failure state: "Online," "Rebuild" (someone initiated a raid rebuild), or "Degraded" (the disk may fail soon; you may want to attempt a raid rebuild before it fails).

DNAS (Managed-Volume Software) Failure

dnasForceRecovery (135) - A managed volume encountered a metadata corruption that obligated it to restart. All other volumes in the same volume-group domain are run by the same process, so they have also restarted.

Clients may not perceive any loss of service, but this trap may indicate a growing problem. Use the collect diags command to collect diagnostic information and send it to F5 Support.

You can configure this trap as an email event (see email-event). It is part of the "storage" event group.

dnasInstanceStartupFailure (136) - An NFS front-end service failed to fully start up, and is now retrying every few seconds. If the startup process succeeds later, the service software writes a "Resuming startup..." message in the syslog. You can use tail logs syslog follow to watch the syslog from the CLI. If the "Resuming startup..." message does not appear after several minutes, you may need to reload the ARX; contact F5 Support for guidance in this case.

The show nfs-service command shows the current state of all NFS services on the ARX.

DNS Servers for Dynamic DNS

Each of these traps can be configured as an email event (see email-event). They are part of the "network" event group.

dnsServerOffline (140) - The ARX has detected that a DNS server has gone offline. The IP address of the failed server is in the trap.

We recommend redundant DNS servers for each Active-Directory (AD) domain. If at least one is running, CIFS services in the domain can continue their DNS registrations when one server fails. Windows clients can then connect to the CIFS service through all DNS aliases. You can use the name-server command to identify each DNS server. After you add a new name server, you can use dynamic-dns update to immediately retransmit all DNS updates.

dnsServerOnline (141) - A DNS server that was previously declared offline (with the dnsServerOffline trap) has come back online.

dnsServerRemove (142) - A DNS server has been removed from the ARX configuration. From the CLI, you can use no name-server to remove a DNS server.

dnsNameUpdateRaise (143) - A CIFS service attempted to add or remove a DNS "A" record and failed. It tried at every name server assigned to the current Active-Directory (AD) domain. It retries once per minute, but it only sends another trap on success (dnsNameUpdateClear) or on cancellation (dnsNameUpdateCancel). Windows clients in the domain may not be able to connect to the CIFS service until this issue is resolved. We recommend that each AD domain have multiple DNS servers; you can use the name-server command to add more to the configuration. Once you correct the problem, you can use dynamic-dns update to immediately try to add and/or remove all "A" records.

dnsNameUpdateClear (144) - A previously-failed DNS registration has now succeeded. The failed registration should have been noted with an earlier dnsNameUpdateRaise trap.

dnsNameUpdateCancel (145) - Someone used no dynamic-dns to remove a DNS hostname that was never successfully registered. The failing registration should have been noted with an earlier dnsNameUpdateRaise trap.

Down-Rev AD Forest

Each of these traps can be configured as an email event (see email-event). They are part of the “cifs” event group.

downRevAdForestLevelRaise (148) - A CIFS service joined a Windows Domain (domain-join) with constrained delegation, but the forest-functional level of the domain’s AD forest is below Windows 2003. *Constrained Delegation* is a Windows 2003 feature that allows the ARX service to delegate its CIFS services to a limited number of back-end filers, so that clients can authenticate once to the ARX service and be trusted at all of the filers behind it. Constrained delegation is recommended for all CIFS services on the ARX. If the forest functional level is below Windows 2003, some of the forest’s domains may not support constrained delegation: CIFS clients from those domains may not be able to use the ARX service. Check your AD configuration and confirm that the down-rev domains do not have any clients that require the service, or raise those domains to a functional level of at least Windows 2003.

Note that the local domain’s functional level must be at Windows 2003 or above, or the domain-join command would have failed. CIFS clients in the local Windows domain should be able to successfully authenticate to the ARX service.

downRevAdForestLevelClear (149) - The AD forest-functional level just rose to Windows 2003 or greater, so all domains in the AD forest can now support constrained delegation. All clients from all domains in the forest can now successfully authenticate to the ARX CIFS service. This clears the alarm condition raised by an earlier ’downRevAdForestLevelRaise’ trap.

Down-Rev NTLM Authentication Server

Each of these traps can be configured as an email event (see email-event). They are part of the “cifs” event group.

downRevNtlmAuthServerRaise (150) - An NTLM Authentication Server on one of your DCs is running an older software release than the ARX. (The NTLM authentication server is also called an ARX Secure Agent, or *ASA*.) Specifically, the ARX software supports NTLMv2, and one of its namespaces has NTLMv2 configured (with the cifs authentication ntlmv2 command), but the ASA is running an older version of software that only supports NTLM. At least one ASA must run Release 5.01.000 or later for any namespace to support NTLMv2 authentication. We recommend upgrading all ASAs in your network.

Please upgrade the DC (shown in the trap) with the latest ASA software. The latest ASA software is available from the ARX GUI. Refer to *ARX® Secure Agent Installation Guide* for complete upgrade instructions.

downRevNtlmAuthServerClear (151) - A formerly down-Rev ASA has come online at the same software release as the ARX. This indicates that the ARX software can support all of its newest NTLM features (such as NTLMv2) when it uses this ASA. This clears the alarm condition raised by an earlier ’downRevNtlmAuthServerRaise’ trap.

Fans

You can add either of these traps to an email event (see email-event). They are part of the “chassis” event group.

fanFail (160) - The fans have failed. Specifically, the state has changed to “absent,” “control failed” (the fan controller has failed), or “failed.” You can replace the entire control plane in an ARX-4000, as described in the *ARX®–4000 Hardware Installation Guide*. The smaller platforms do not have replaceable fans and must be entirely replaced. Their Hardware Installation manuals contain ARX-replacement procedures.

fanStatus (161) - The fans have changed state to “good” from a former failed state.

Filers and Servers

filerErrorsRaise (172) - The stats monitor process has detected that a back-end filer has suddenly started returning a large number of errors. The filer and share are both identified in the trap text. The stats monitor counts errors from all filers, and this trap appears if the error counts increase significantly from their moving average, and if the increase persists over some number of samples. You can use the moving-average command to set two thresholds for this trap: the percentage increase that is significant enough to merit a trap, and the number of samples that are required.

This trap never appears unless you enable stats-monitor traps with the trap command. To enable stats-monitor traps for NFS filers, use notify filer-share nfs followed by trap. To enable stats-monitor traps for CIFS filers, use notify filer-share cifs followed by trap.

You can add this trap to an email event (see email-event). It is part of the “statsmon” event group.

filerErrorsClear (173) - A filer that was formerly returning a higher-than-average number of errors has returned to an error count that is not significantly above the moving average. The filer is identified in the trap text. This may indicate that the filer’s number of errors has decreased, or it may indicate that the increased error count has remained steady for a large number of samples, or a combination of the two. In any case, the error counts have been fairly consistent over a large number of samples. For some number of error-count samples, the error count has not been significant enough to merit an alarm, as determined by the settings of the moving-average command.

This clears the alarm that was formerly raised by a ‘filerErrorsRaise’ trap.

As with the filerErrorsRaise trap, this trap never appears unless you enable stats-monitor traps with the trap command. To enable stats-monitor traps for NFS filers, use notify filer-share nfs followed by trap. To enable stats-monitor traps for CIFS filers, use notify filer-share cifs followed by trap.

You can add this trap to an email event (see email-event). It is part of the “statsmon” event group.

filerSlowRaise (170) - The stats-monitor process has detected that a back-end filer has suddenly slowed. The filer and share are both identified in the trap text. Round-trip times (RTTs) are measured for all communication between the ARX and its filers, and this trap appears if the times increase significantly from their moving average, and if the increase persists over some number of RTT samples. You can use the moving-average command to set two thresholds for this trap: the percentage increase that is significant enough to merit a trap, and the number of RTT samples that are required.

This trap never appears unless you enable stats-monitor traps with the trap command. To enable stats-monitor traps for NFS filers, use notify filer-share nfs followed by trap. To enable stats-monitor traps for CIFS filers, use notify filer-share cifs followed by trap.

You can add this trap to an email event (see email-event). It is part of the “statsmon” event group.

filerSlowClear (171) - A filer that was formerly slow has returned to a round-trip time (RTT) that is not significantly above the moving average. The filer is identified in the trap text. This may indicate that the filer’s RTT time has decreased, or it may indicate that the increased RTT has remained steady for a large number of samples, or a combination of the two. In any case, the RTTs have been fairly consistent over a large number of samples. For some number of RTT samples, the RTT has not been significant enough to merit an alarm, as determined by the settings of the moving-average command.

This clears the alarm that was formerly raised by a ‘filerSlowRaise’ trap.

As with the filerSlowRaise trap, this trap never appears unless you enable stats-monitor traps with the trap command. To enable stats-monitor traps for NFS filers, use notify filer-share nfs followed by trap. To enable stats-monitor traps for CIFS filers, use notify filer-share cifs followed by trap.

You can add this trap to an email event (see email-event). It is part of the “statsmon” event group.

filerCapacity (180) - reserved for future use.

filerAccessDenied (181) - The policy engine does not have adequate privileges to change file attributes on a back-end filer. To migrate a file from one filer to another, the policy engine must duplicate the source file’s attributes as well as its name and path. The filer returned a

“STATUS_ACCESS_DENIED” reply when the ARX tried to set the destination file’s CIFS attributes, and/or a similar reply when setting the file’s NFS attributes.

For CIFS, this indicates that the namespace requires Windows credentials with more control at the destination filer. The namespace uses its assigned *proxy user* (username and password) for its Windows credentials. The proxy-user credentials must belong to the Backup Operator’s group at this filer. If necessary, you can use the proxy-user command to change the credentials themselves, or use proxy-user (gbl-ns) to select new proxy-user credentials for the volume’s namespace.

For NFS, check your back-end filer configuration: the back-end share should allow *root* access to all of the ARX’s proxy IP addresses. Use the show exports command examine all permission settings at the filer. Use the show ip proxy-addresses command to list all configured proxy IP addresses.

Firmware

You can configure each of these traps as an email event (see email-event). They are part of the “chassis” event group.

Firmware is low-level software that is delivered in the same release file that hold the ARX software.

firmwareUpgradeInitiated (182) - An administrator entered the firmware upgrade command to start upgrading the ARX firmware. Any firmware upgrade ends with an ARX reboot, which may trigger one or more cpuHalt traps. The cpuHalt traps are expected for many firmware upgrades.

This trap is informational.

firmwareMismatchRaise (183) - The ARX software detected that the running software release is different from the running firmware release. This conflict limits the capabilities of the ARX software, and may result in system instability.

Use the show firmware upgrade command to confirm the mismatch, then use the firmware upgrade command to install the matching firmware. This results in an ARX reboot and may trigger one or more cpuHalt traps. The cpuHalt traps are expected for many firmware upgrades.

firmwareMismatchClear (184) - Formerly mismatched firmware has now been updated. This clears the alarm condition raised by the ’firmwareMismatchRaise’ trap.

Gateways for Static Routes

You can add any of these traps to an email event (see email-event). They are part of the “network” event group.

gatewayOffline (185) - The ARX can no longer reach the IP address in this trap, a gateway for a static route. This indicates a serious connectivity issue. Check the connection to the gateway and correct the problem as soon as possible. The trap message indicates whether the gateway is an “Out of Band Management” gateway (connected to the MGMT interface) or a “client” gateway for the client/server ports. You can use the ping and expect traceroute commands to verify connectivity from the ARX.

You can use the ip route CLI command to create or edit a static route. To see all of the static routes on the ARX, use the show ip route command.

gatewayOnline (186) - A gateway that was formerly unreachable is now reachable. The IP address of the gateway appears in the trap text. This trap clears the alarm condition raised by the gatewayOffline trap.

gatewayRemove (187) - An administrator has used the no ip route command to remove a static-route gateway. The IP address of the deleted gateway appears in the trap text. This trap clears the alarm condition raised by the gatewayOffline trap.

HA (Redundancy)

haPairClusterTransition (210) - reserved for future use.

haPairClusterOffline (211) - The peer node failed. Contact F5 Support if you receive this trap. The ARX that sends this trap is currently active.

haPairClusterOnline (212) - The peer node rejoined the cluster. The ARX that sends this trap is currently active, and the peer node that came back online is in the backup role.

haPairFormation (190) - Two ARXes are forming a redundant pair.

haPairNsmDoubleFault (193) - NSM processors run in redundant pairs on the same switch. Both processors in a redundant pair have failed and nsm recovery is not configured, or a pair of redundant processors failed at the same time. In either case, some clients cannot reach their storage services. In an effort to recover, the switch is rebooting. If this happens frequently, you may need to replace the NSM.

haPairQDiskFreeSpaceWarningRaise (192) - Quorum Disk free space is low. This condition can cause redundancy to function improperly. You can directly access the quorum-disk filer to clear some disk space.

You can configure this trap as an email event (see email-event). It is part of the “redundancy” event group.

haPairQDiskFreeSpaceWarningClear (191) - Quorum Disk free space has returned to an acceptable level.

You can configure this trap as an email event (see email-event). It is part of the “redundancy” event group.

haPairQDiskTransition (200) - This trap is currently unsupported.

haPairQDiskOffline (201) - The quorum disk failed. This is a serious condition that you should address immediately. You can use show exports to check the network connection to the quorum-disk filer, show redundancy quorum-disk to view historical data about the quorum-disk, and the quorum-disk command (on both peers) to assign a new, more-reliable quorum disk to the redundant pair.

haPairQDiskOnline (202) - The quorum disk came back online after a previous failure. This clears the alarm condition set by the haPairQDiskOffline trap.

haPairStallEvent (220) - The ARX (or its peer) rebooted and a redundancy election began, but the election was inconclusive. The ARX is waiting for a short time, then it will retry the quorum election. These conditions can cause an inconclusive election:

- The ARX cannot reach its peer or the Quorum Disk. This may be because the ARX is still booting, and its network interfaces are not yet active.
- The peer has a higher Epoch number, but it is currently offline. This ARX refuses to start because its peer has processed namespace transactions while it was offline; these transactions are lost if it takes control. If the peer is never coming back, you can use the redundancy force-active command to force this switch to take control.

haPairVersionAutoSyncRaise (223) - The backup peer is running an older software release, so a managed volume could not perform an auto-sync operation. An *auto-sync* operation occurs when a client fails to access a file that was moved at the filer (possibly by an anti-virus application); a managed volume with auto sync files is supposed to react to the failure by scanning the back-end filer and updating its metadata as needed. The metadata update cannot occur if the redundant peer has an earlier version of metadata, so the volume drops the auto-sync operation.

To allow future auto-syncs to proceed, either upgrade the backup peer to the active peer's software release, or reload the active peer so that the backup peer takes control. An auto sync can proceed if the backup peer has the same software release or a newer one.

You can configure this trap as an email event (see email-event). It is part of the "redundancy" event group.

haPairVersionAutoSyncClear (224) - Auto-sync operations (described above) can now occur. Either the backup peer was upgraded to the same software release, or the peer with the lower software release just took control of the redundant pair.

As above, you can configure this trap as an email event (see email-event). It is part of the "redundancy" event group.

haPairVersionMismatchRaise (227) - The trap is the result of a specific set of circumstances:

1. the active peer is running an older software release than the backup peer;

2. an administrator invoked an import, nsck, or sync operation on the active peer (not recommended during a version mismatch);
3. a failover occurred before the operation completed; and
4. the operation could not continue on the newly-active peer.

The operation cannot complete because the active peer is now the one that is running a newer software release. A change to metadata in the new release cannot be mirrored on the backup peer's older release, so metadata-changing operations are not allowed.

To allow the import/nsck/sync operation to complete, either upgrade the backup peer to the active peer's software release, or reload the active peer so that the backup peer takes control. You can make metadata changes only if the backup peer has the same software release or a newer one.

As above, you can configure this trap as an email event (see email-event). It is part of the "redundancy" event group.

haPairVersionMismatchClear (226) - All blocked import, nsck, and sync operations (described above) are now proceeding. Either the backup peer was upgraded to the same software release, or the peer with the lower software release just took control of the redundant pair.

As above, you can configure this trap as an email event (see email-event). It is part of the "redundancy" event group.

Kerberos

You can add any of these traps to an email event (see email-event). They are part of the "cifs" event group.

kerberosDCOffline (230) - A domain controller (DC) for an Active-Directory (AD) domain has gone offline. Check the DC for connectivity issues; the IP address of the DC is in the trap. You can use show active-directory to see the full AD forest, including this DC.

kerberosDCOnline (231) - A domain controller (DC) for an Active-Directory (AD) domain has changed state from "offline" to "online." This is one of the DCs in the local Active-Directory forest, identified in the trap by its IP address. As mentioned above, you can use show active-directory to see the full AD forest, including this DC.

kerberosDCRemove (229) - An administrator used the no forest-root, no child-domain, or no tree-domain command to remove a domain controller (DC) from an Active-Directory (AD) forest configuration. This is the AD forest that is known to the ARX. You can use show active-directory to see the remaining AD-forest configuration. If the ARX sent a kerberosDCOffline trap for this DC earlier, this trap clears the alarm condition for that trap.

kerberosCacheRaise (232) - The Kerberos processes keep an updated cache of tickets granted to clients. This trap indicates that the cache is filling up. The trap appears if the cache is 90%, 95%, 98%, or 100% full; each trap indicates the degree of fullness. Kerberos cannot grant tickets to any Windows clients if the cache fills to 100%. Contact F5 if this occurs. You can use show cifs-service kerberos-tickets to view the current tickets in the cache.

kerberosCacheClear (233) - The Kerberos-ticket cache has crossed back over a threshold; it is now less full than when the previous kerberosCacheRaise trap appeared. The crossed threshold appears in the trap text.

Kernel

kernelNMIError (235) - The kernel received a Non-Maskable Interrupt (NMI) error from the memory controller or another hardware device. This may be accompanied by one of the following traps:

- ramECCCorrectableError indicates that Random Access Memory (RAM) controller found a write error, called a RAM ECC error, and can correct it.
- ramECCError indicates that the memory controller found a RAM ECC error that it cannot correct.
- systemBusError means that there is a communication problem between a processor and memory controller (or other hardware device).

Follow the instructions for the above traps if you see one of them. In any case, contact F5 Support if you see this trap.

You can configure this trap as an email event (see email-event). It is part of the “chassis” event group.

Licensing

You can add any of these traps to an email event (see email-event). They are part of the “chassis” event group.

licenseExpiredRaise (241) - The software license on an ARX has expired. Clients can no longer use the storage services on the ARX, and you can no longer edit the storage configuration. You can re-activate a trial license a limited number of times with the license activate or license activate file command. If that fails, contact F5 Support to extend the license-evaluation period or extend the contract, then run one of the above commands again.

licenseExpiredClear (242) - An administrator ran the license activate or license activate file command to reactivate an ARX license. This clears the alarm condition raised by the ’licenseExpiredRaise’ trap.

licenseNotFoundRaise (243) - An ARX discovered (while booting) that it has no software license. Clients cannot use any storage services on the ARX, and you cannot edit the storage configuration. Use the license activate or license activate file command to activate your license.

licenseNotFoundClear (244) - An administrator ran the license activate or license activate file command to activate an ARX license. This clears the alarm condition raised by the ’licenseNotFoundRaise’ trap.

licensePendingExpirationRaise (245) - The software license on an ARX will expire soon. The time remaining for the license is included in the trap text. After the license expires, clients can no longer use the storage services on the ARX, and you can no longer edit the storage configuration. You can re-activate a trial license a limited number of times with the license activate or license activate file command. If that fails, contact F5 Support to extend the license-evaluation period or extend the contract, then run one of the above commands again.

licensePendingExpirationClear (246) - An administrator ran the license activate or license activate file command to reactivate an ARX license. This clears the alarm condition raised by the ’licensePendingExpirationRaise’ trap.

licenseProtocolQtyRaise (247) - The ARX is running more network-storage protocols than its license supports. The network-storage protocols supported are NFS and CIFS; one or more nfs front-end services uses the license for one protocol, and one or more cifs front-end services uses the license for another protocol. If your license supports only 1 protocol, you are not licensed for both service types.

You can clear this alarm condition by acquiring an add-on license for an additional protocol. Contact your F5 Sales representative to acquire an add-on license for additional protocols, then run the license activate or license activate file command to activate the add-on license.

licenseProtocolQtyClear (248) - Formerly, more network-storage protocols (NFS and/or CIFS) were in use than the ARX license allowed. Now you have adequate licensing for the current number of network-storage protocols. Either an add-on license increased the limit, or the number of supported protocols was reduced. This clears the alarm condition raised by the ’licenseProtocolQtyRaise’ trap.

licensePlatformLimitRaise (249) - The ARX license allows for a higher limit than the ARX can support. The specific licensed feature or limit is called out in the trap text.

Contact F5 Support if you receive this trap; it indicates that the current license is incorrect and should be renewed after it is corrected. After the issue is corrected at F5, use the license activate or license activate file command to re-activate your license.

licensePlatformLimitClear (251) - Previously, the license allowed higher limits than the ARX could support. Now, the license limits are all supportable by the host ARX. This clears the alarm condition raised by the ’licensePlatformLimitRaise’ trap.

licenseHaPeerDifferentRaise (252) - The license on the current ARX is different from the license on its redundant peer. The licenses must match so that the redundant peer can take control of all storage services after a failover. For a complete listing of all the limits that differ between the two licenses, you can use the show redundancy license command.

If this is a trial or evaluation license and the only difference is the license end dates, the licenses were activated more than 1 day apart from each other. You need to re-acquire both licenses and activate them both on the same day.

In any case, contact F5 Support if you receive this trap. F5 Support can replace the errant license or licenses. After you receive a new license, run the license activate or license activate file command to activate it on the peer where it was incorrect.

licenseHaPeerDifferentClear (253) - The current ARX has precisely the same licensed limits as its redundant peer. The backup peer is now fully licensed to take over all the services of the active peer. This clears the alarm condition raised by the 'licenseHaPeerDifferentRaise' trap.

licenseHaPairDisabledRaise (254) - In a redundant pair of ARX devices, one peer is licensed and the other peer is unlicensed. The redundant pair cannot form until both peers are licensed. This trap is normal for a situation where you are upgrading a redundant pair from a release that does not support ARX licensing to a later release that does. The ARX will send a licenseHaPairDisabledClear trap after the peer is upgraded and licensed.

After you upgrade the down-rev peer, you can use the license activate or license activate file command to activate the license.

licenseHaPairDisabledClear (255) - Both ARX devices in a redundant pair have fully activated licenses, so they can successfully pair. This clears the alarm condition raised by the 'licenseHaPairDisabledRaise' trap.

Logging Daemon (for the syslog)

You can add either of these traps to an email event (see email-event). They are part of the “chassis” event group.

loggingFailureRaise (238) - The internal logging daemon, which filters system messages and writes them to the syslog, has failed. It should restart momentarily; contact F5 Support if the corresponding 'loggingFailureClear' trap does not appear after five minutes.

loggingFailureClear (239) - The internal logging daemon, which filters system messages and writes them to the syslog, has restarted. This clears the alarm condition raised by the 'loggingFailureRaise' trap.

Metadata

metaDataFailure (240) - While a volume was first coming online, it discovered a configuration problem at the named metadata share. The filer host is evidently failing to write all volume metadata to stable storage. This means that all volumes that use this share are offline, as well as any other volumes that are running on the same volume-group as any of those volumes; use show volume-group to find the volume group(s) and volume(s) affected by each metadata outage.

The correct metadata-filer configuration is described in *Performance and Availability Requirements*, on page 1-29 of the *ARX® Site Planning Guide*. You can go to the metadata filer (identified in the trap) and change its configuration as needed, or you can use the no metadata share and metadata share commands (or their GUI equivalents) to switch to a new metadata filer and share.

metaDataFreeSpaceThresholdRaise (260) - A metadata share just dropped below a warning threshold, 512 M, 256 M, or 128 M. If it drops below the minimum threshold, 128 M, all volumes that use the share go offline. Use show namespace all to find all metadata shares in use by all volumes in the system. Access the volume's metadata share directly and clear some space, or use nsck ... migrate-metadata to migrate the volume's metadata to a larger share.

You can configure this trap as an email event (see email-event). It is part of the "metadata" event group.

metaDataFreeSpaceThresholdClear (250) - A metadata share just rose above 512 MegaBytes, which is considered ample free space.

As above, you can configure this trap as an email event (see email-event). It is part of the "metadata" event group.

metaDataOffline (270) - A metadata share has gone offline. (The filer IP and share name is identified in the trap.) This means that all volumes that use this share are offline, as well as any other volumes that are running on the same volume-group as any of those volumes; use show volume-group to find the volume groups(s) and volume(s) affected by each metadata outage. If this outage was unplanned, take immediate steps to bring the metadata share back online.

As above, you can configure this trap as an email event (see email-event). It is part of the "metadata" event group.

metaDataOnline (280) - A metadata share, identified in the trap, has come back online. This clears the alarm condition raised by the metaDataOffline trap.

As above, you can configure this trap as an email event (see email-event). It is part of the "metadata" event group.

Metalog

Namespace software and networking software record important log information, called *metalog* data, to be used by a redundant peer in the event of a failover. These traps all pertain to metalog storage.

metaLogFail (290) - The system encountered a metalog failure. Contact F5 Support if you receive this trap.

metaLogLatencyRaise (291) - The ARX-1500 and ARX-2500 store their metalog data on internal disk partitions, both on the active ARX and its redundant peer. This trap indicates that the latency for storing the metalog data (either locally or at the redundant peer) has risen above an acceptable threshold. You can use the show metalog usage command to view the metalog-storage latency over time.

The ARX software continues to monitor metalog latency and lowers this alarm condition if the latency falls back below the threshold. The metaLogLatencyClear trap clears the alarm. Contact F5 Support if this alarm condition persists.

An ARX-1500 or ARX-2500 raises this alarm at least once during a software upgrade (see boot system), then lowers it when the upgrade is complete. This is standard. The corresponding metaLogLatencyClear trap(s) should appear within five minutes to clear the alarm(s).

You can configure this trap as an email event (see email-event). It is part of the “chassis” event group.

metaLogLatencyClear (292) - The metalog-storage latency has improved to an acceptable level. This clears the alarm condition raised by the ’metaLogLatencyRaise’ trap.

As above, you can configure this trap as an email event (see email-event). It is also part of the “chassis” event group.

metalogResilverTmo (293) - The metalog resilvering process timed out and restarted. This trap can occur for redundant peers that are separated by a great distance, or due to other causes for high latency. You can use the show redundancy metalog command to monitor the next resilvering process, and you can use resilver-timeout to increase the timeout threshold.

metalogResilverClear (294) - The metalog resilvering process completed successfully after a former timeout. Now the resilvering occurs incrementally; as the namespace software on the active peer records each metalog record, it also copies the packet to its backup peer.

This clears the alarm condition raised by the ’metalogResilverTmo’ trap.

Modules

You can add either of these traps to an email event (see email-event). They are part of the “chassis” event group.

moduleFail (300) - A module (identified in the trap) has failed. You can replace the entire control plane (slot 1) or data plane (slot 2) in an ARX-4000, as described in the *ARX®–4000 Hardware Installation Guide*. On an ARX-2000, you can replace modules as described in its Hardware Installation manual, the *ARX®–2000 Hardware Installation Guide*. The smaller platforms do not have replaceable modules and must be entirely replaced. Their Hardware Installation manuals contain ARX-replacement procedures.

moduleStatus (310) - A chassis module changed from a failed state to a good state.

NFS Access Errors

These traps indicate that an NFS service gave one of its clients an access error (typically NFS3ERR_ACCES or NFSERR_ACCES). This can only occur in an NFS service where someone has used the offline-behavior deny-access command or its GUI equivalent.

You can add either of these traps to an email event (see email-event). They are part of the "storage" event group.

nfsAccessErrorRaise (316) - An NFS client has attempted to access the storage on an offline filer, and the ARX returned an access error to that client. This trap only appears once for a given offline-filer share. The trap identifies the filer's IP address and the name of the unavailable filer share. You can use the ping and expect traceroute commands to check connectivity to the back-end filer, and you can use show exports to test whether or not the ARX can communicate to the filer through NFS.

nfsAccessErrorClear (315) - A filer has come back online, after at least one NFS client has received an access error. This clears the alarm condition raised by the 'nfsAccessErrorRaise' trap.

NIS

nisUpdateStart (344) - A NIS update has begun. A NIS update refreshes the switches cache of NIS netgroups. This process starts when an administrator configures a new NIS domain (with nis domain) or uses the nis update command.

nisUpdateComplete (342) - The switch has successfully updated its local cache of NIS netgroups. This update occurs whenever a NIS domain is first configured, or when someone uses the nis update command.

nisUpdateFail (343) - The switch has failed to update its local cache of NIS netgroups. For details, refer to the report from the nis update command.

NSCK

nsckDestageStatus (360) - An nsck ... destage is either starting or just completed. The trap includes the name of the namespace and volume that was destaged. The text indicates whether or not the destage operation is starting or completing.

nsckRebuildStatus (390) - An nsck ... rebuild is either starting or just completed. The trap includes the name of the namespace and volume that was rebuilt. The text indicates whether or not the rebuild operation is starting or completing.

nsckReportLogicalScan (370) - reserved for future use.

nsckReportPhysicalScan (380) - reserved for future use.

nsckReportReimport (400) - The nsck utility is rebuilding one or more managed volumes, named in the trap text. This is an unscheduled rebuild, due to the discovery of a corruption in the volume's database. The rebuild operation is the same as the one invoked by the nsck ... rebuild command.

You can configure this trap as an email event (see email-event). It is part of the "nsck" event group.

nsckReportStatus (410) - An nsck ... report inconsistencies command finished; this trap contains the final status of the report.

nsckMdMigrateStatus (365) - An nsck ... migrate-metadata operation just started or finished, as indicated by the trap's text message. The trap also includes the name of the namespace and volume whose metadata is migrating (or finished migrating) to a new external share.

The volume is offline while its metadata migrates; each of its shares sends a shareOffline trap when the migration starts and a shareOnline trap when it returns to service.

nsckVolGroupMigrateStatus (366) - An nsck ... migrate-volume operation just started or finished, as indicated in the trap text. This operation migrates a volume from one volume-group to another. The trap includes the name of the volume that is (or just finished) migrating.

The volume is offline during the migration; each of its shares sends a shareOffline trap when the migration starts and a shareOnline trap when it returns to service.

NSCK Repair (obsolete)

The nsck ... repair command has been replaced by sync files. These traps are in the MIB, but they are no longer supported.

namespaceRecovery (320) - An administrator started an nsck repair operation.

namespaceRecoveryComplete (330) - An nsck repair operation succeeded.

namespaceRecoveryFail (340) - An nsck repair operation failed.

NSM (Network Services Module)

nsmStandby (411) - An NSM processor (identified in the trap) is now in a standby state. Its peer processor is managing traffic for both processors. If the peer processor fails, this processor takes control and handles the network traffic for both processors.

You can configure this trap as an email event (see email-event). It is part of the "chassis" event group.

nsmStandbyClear (412) - An NSM processor (identified in the trap) is now actively processing packets. It was previously in a standby state; its peer processor has failed and it is now processing network traffic for both processors.

You can configure this trap as an email event (see email-event). It is part of the “chassis” event group.

nsmClientFenceRaise (413) - This trap is currently unsupported.

nsmClientFenceClear (414) - This trap is currently unsupported.

nsmWarmRestart (424) - An NSM processor (identified in the trap) has restarted after a software failure. This is a restart of a single core on the hardware CPU, and is recommended over restarting the entire CPU; you can use the nsm warm-restart command to set this failure-recovery method for your network cores. If the same network core fails three times in 24 hours or less, the full CPU reboots and an “nsmStandby” trap appears.

The warm restart produces a small core-memory file that you can examine with the show cores command. You can also use the collect diags command to send this file and other diagnostic information to F5 Support.

You can configure this trap as an email event (see email-event). It is part of the “chassis” event group.

NSM Resources

You can add either of these traps to an email event (see email-event). They are part of the “chassis” event group.

nsmResourceThreshold (415) - An NSM processor has used over 80% of a critical resource, where the specific resource is named in the trap. The system re-issues the trap if the processor exceeds 90% of the resource. The system re-issues this trap again if it needs to *exceed* 100% of the resource. The trap identifies the processor and exhausted resource, and shows how much of the resource is used (80%, 90%, or >100%).

Contact Customer Service if this trap appears; they can explain the nature of the depleted resource, and can formulate a plan to address the issue.

nsmResourceThresholdClear (416) - An NSM processor was previously using greater than 80, 90, or >100% of a critical resource, but is now using at least 10% below one of those marks (90%, 80%, or 70%). The trap shows the threshold of the cleared trap (80%, 90%, or >100%), the processor, and the type of resource that is freeing up.

NTLM Authentication Server (or ASA)

Each of these traps can be configured as an email event (see email-event). They are part of the “cifs” event group.

ntlmAuthServerOfflineRaise (346) - An NTLM Authentication Server, identified in the trap by its IP address, stopped responding to NTLM queries from the ARX. The NTLM Authentication Server is a DC that runs the ARX Secure Agent (*ASA*) application. Using the ASA, the ARX software can challenge an NTLM client once for his or her credentials and then silently repeat the authentication for multiple back-end filers. Each ASA facilitates NTLM authentications for clients in one Windows domain. If all the ASAs for a given domain go offline, clients from that domain cannot NTLM-authenticate to ARX services.

To clear this alarm condition, check the operational status of the ASA as well as the connection to the DC . The show ntlm-auth-server command shows the operational status; add the detailed keyword to show the IP port used for ASA connections. Use this output (together with the ASA applet) to confirm that the ARX and the ASA use the same IP port and password. You can also use the ping and expect traceroute commands to verify connectivity between the DC and the ARX.

For more details about the ASA, including installation instructions and instructions for using its applet, refer to *ARX® Secure Agent Installation Guide*.

ntlmAuthServerOfflineClear (347) - A formerly unreachable ASA is now responding to NTLM queries. This clears the alarm condition that was raised by an earlier ’ntlmAuthServerOfflineRaise’ trap.

NTLM DC

Each of these traps can be configured as an email event (see email-event). They are part of the “cifs” event group.

noNtlmAuthDCRaise (348) - No DC is answering Netlogon requests for a particular CIFS service. Because of this, the CIFS service’s clients cannot authenticate with NTLM or NTLMv2.

To clear this alarm condition, check the connection to the DCs in the service’s domain, as well as the operational status of the DCs. The domain name appears in the trap. The show active-directory status command lists all the DCs in the forest and shows their operational status. Use the ping and expect traceroute commands to verify connectivity between the domain’s DCs and the ARX. If necessary, go to the DCs and restart Netlogon service.

noNtlmAuthDCClear (349) - A CIFS service formerly could not make a Netlogon connection to any DC in its domain; now it has successfully established a Netlogon connection with one of its DCs. The CIFS service can therefore authenticate its NTLM and NTLMv2 clients. This clears the alarm condition that was raised by an earlier ’noNtlmAuthDCRaise’ trap.

NTP

ntpSync (350) - The NTP status changed. See the documentation for show ntp status to interpret the NTP status in the trap.

ntpUnreachable (351) - The ARX lost contact with an NTP peer. The IP address of the peer is identified in the trap. You can use the ping and expect traceroute commands to verify connectivity to the NTP server.

You can configure this trap as an email event (see email-event). It is part of the "network" event group.

ntpReachable (352) - A previously-unreachable NTP server, identified with an earlier ntpUnreachable trap, is now reachable again.

As above, you can configure this trap as an email event (see email-event). It is part of the "network" event group.

Number of Files is Too High

These traps alert you to a volume that is running out of file credits. A volume requires one *file credit* for each of its files and directories. Clients cannot add any more files or directories after all of the volume's file credits are used. For more information on file credits, see the documentation for the auto reserve files command.

You can add any of these traps to an email event (see email-event). They are part of the "storage" event group.

numberOfFilesWarnRaise (354) - A volume is 80% full. That is, the volume has used 80% of its maximum file credits. Clients cannot create any new files if the volume uses all of its file credits. To clear this alarm condition, use any combination of the following methods:

- Connect to the volume through a front-end service and remove unused files.
- Use the reserve files command to increase the number of file credits for this volume.
- If auto reserve files is enabled for the volume, the volume may automatically increase the maximum file credits.

numberOfFilesWarnClear (355) - A volume that previously was above 80% utilization of its files has fallen below 80%. This clears the alarm raised by the 'numberOfFilesWarnRaise' trap.

numberOfFilesWarnCancel (356) - A volume that previously was above 80% file utilization has been removed. (You can use the remove namespace namespace volume vol-path command to remove a volume.) As above, this clears the alarm raised by the 'numberOfFilesWarnRaise' trap.

numberOfFilesCriticalRaise (357) - A volume is 90% full. That is, the volume has used 90% of its maximum file credits. Clients cannot create any new files if the volume uses all of its file credits. To clear this alarm condition, use any combination of the methods described above for ‘numberOfFilesWarnRaise.’

numberOfFilesCriticalClear (358) - A volume that previously was above 90% utilization of its files has fallen below 90%. This clears the alarm raised by the ‘numberOfFilesCriticalRaise’ trap.

numberOfFilesCriticalCancel (359) - A volume that previously was above 90% file utilization has been removed. (You can use the remove namespace namespace volume vol-path command to remove a volume.) As above, this clears the alarm raised by the ‘numberOfFilesCriticalRaise’ trap.

numberOfFilesFullRaise (361) - A volume is 100% full. That is, the volume has used all of its maximum file credits. Clients cannot create any new files or directories in this volume. To clear this alarm condition, use any combination of the methods described above for ‘numberOfFilesWarnRaise.’

numberOfFilesFullClear (362) - A volume that previously was full has fallen below 100%. This clears the alarm raised by the ‘numberOfFilesFullRaise’ trap.

numberOfFilesFullCancel (363) - A volume that previously was above 100% file utilization has been removed. (You can use the remove namespace namespace volume vol-path command to remove a volume.) This clears the alarm raised by the ‘numberOfFilesFullRaise’ trap.

NVRAM

nvramBatteryDegraded (418) - The battery is degraded for NVRAM, a memory chip for storing important namespace-transaction logs. This presents a potential problem for failure recovery; current processing is unaffected. The battery is no longer guaranteed to last for 72 hours after the ARX loses power. After a power outage, in-flight namespace transactions may not be recoverable on this switch. Contact F5 personnel to correct this as soon as possible.

You can configure this trap as an email event (see email-event). It is part of the “chassis” event group.

nvramBatteryDegradedClear (417) - The NVRAM battery rose back above the “degraded” threshold described above. The battery is now guaranteed to last for at least 72 hours.

You can configure this trap as an email event (see email-event). It is part of the “chassis” event group.

nvramBatteryFail (419) - The NVRAM battery failed. This presents a problem for failure recovery; current processing is unaffected. On the next reboot, in-flight namespace transactions will not be recoverable on this switch. Contact F5 personnel to correct this as soon as possible.

You can configure this trap as an email event (see email-event). It is part of the “chassis” event group.

nvramBatteryStatus (420) - The battery-status changed to a non-failure state for NVRAM. The NVRAM is a memory chip for storing important namespace-transaction logs.

This trap can also be configured as an email event (see email-event). It is part of the “chassis” event group.

nvramClear (421) - A user has cleared the NVRAM contents with clear nvr.

nvramNoRefresh (422) - The ARX is being *halted*, which means that it is being rebooted with the NVRAM battery offline. Typically, F5 personnel do this before shipping an ARX from the factory or decommissioning an ARX. When the switch boots later without any data in NVRAM (see below), all volumes will have to re-import all files and all NFS clients will have to re-mount.

nvramNoRefreshBoot (423) - The ARX is being booted without any data in the NVRAM. This is after the switch has been halted, as described above. All configured namespaces (if any) must re-import as they come online. NFS clients must unmount and remount all of the ARX’s NFS exports.

nvramEccError (425) - The Error-Check Circuitry (ECC) found write errors in NVRAM, a memory chip for storing important namespace-transaction logs.

You can configure this trap as an email event (see email-event). It is part of the “chassis” event group.

nvramEccErrorClear (426) - reserved for future use.

nvramNotSaved (427) - The ARX is booting without any data in its NVRAM. All configured namespaces (if any) must re-import as they come online. NFS clients must unmount and remount all of the ARX’s NFS exports.

If this is accompanied by an nvramNoRefreshBoot trap, the condition may have been planned. In any other case, this indicates a serious problem with the NVRAM; contact F5 Support to correct this as soon as possible.

◆ **Note**

NVRAM stores namespace-transaction logs used only for failure recovery. A malfunctioning NVRAM should be corrected quickly to protect against failures, but it does not affect current processing.

You can configure this trap as an email event (see email-event). It is part of the “chassis” event group.

OM Database Usage

These traps pertain to the ARX's configuration database, which manages configuration parameters entered through the CLI or GUI. You can configure either of these traps as an email event (see email-event). They are part of the "chassis" event group.

omTransactionsRaise (430) - The configuration database has kept at least 100,000 transactions in memory over the last 30 minutes, indicating that an internal process is holding a transaction open for an excessive period of time. This can be a serious condition if it persists. Use the collect diags command to collect diagnostic information and send it to F5 Support. Then schedule a maintenance window for the ARX within the next 24 hours. If an omTransactionsClear trap does not appear in 24 hours (see below), reload the ARX.

omTransactionsClear (431) - This clears the omTransactionsRaise trap described above. The number of database transactions in memory has fallen back below 100,000 over the last 30 minutes.

Peer Critical Resources (Redundancy/HA)

You can configure each of these traps as an email event (see email-event). They are part of the "redundancy" event group.

peerCritResRaise (435) - At least one critical resource has failed on the redundant peer for this ARX, so the current ARX is unable to fail over. A critical resource is a static route or share that an administrator has labeled as critical: the critical route command labels a route as critical, the critical command labels a share as critical, and the metadata critical command labels a metadata share as critical. The route to the quorum disk is always critical. If any critical resource fails on the peer, the current ARX cannot fail over.

We strongly recommend resolving this issue to ensure that the redundant ARX is ready to take control in the event of any catastrophic failures. Log into the redundant peer and use the show redundancy critical-services command to find (and then restore) all failed resources.

peerCritResClear (436) - The redundant peer formerly had one or more failed critical resources, but now all of its critical resources are intact. This clears the alarm raised by an earlier 'peerCritResRaise' trap.

Policy

policyRuleAutoMigrateStart (486) - The policy engine has started an automatic migration of files, for the namespace, volume, share, and rule (that is, the share farm) identified in the trap. You can use auto-migrate to configure automatic migration in a share farm.

policyRuleAutoMigrateComplete (487) - The policy engine has finished an automatic migration of files, for the namespace, volume, share, and rule identified in the trap.

policyRuleCompileFail (440) - The policy engine failed to compile a user-defined policy rule. Therefore, it cannot enforce the rule. The rule name is included in the trap.

policyRuleDisable (450) - An administrator has disabled a file-placement or shadow-copy rule, identified in the trap text. Use the place-rule command to create a file-placement rule; use the shadow-copy-rule command to create a shadow-copy rule.

policyRuleEnable (460) - An administrator has enabled a file-placement or shadow-copy rule, identified in the trap text. Use the place-rule or shadow-copy-rule to create one of these rules.

policyRuleFileIgnored (470) - The policy engine is unable to honor the configured policy rules for a specific file. The filename is included in the trap.

policyRuleInlineQueueOverflow (534) - One of the policy engine's internal queues, the inline-notification queue, has filled to capacity for a particular volume. An *inline notification* is a notification from volume software that a client made a change to a file. The policy engine monitors these changes for file-placement rules where inline notify is enabled, or for shadow-copy rules with inline-notify (gbl-ns-vol-shdwcp) enabled. An inline change could newly qualify a file for migration or shadow-copying.

This trap indicates that the queue filled to capacity for a particular volume. The policy engine reacts to this by starting a full, unscheduled scan of the volume's back-end shares. The scan finds all file changes, including any that resulted from missed inline changes. If the volume remains very busy with inline changes during this scan, the queue may fill again and you may get another instance of this trap. This is normal behavior. When client activity subsides on the volume, the scan runs to completion and all of its files are placed and/or copied according to your rules.

Migrate Status for a File-Placement Rule

policyRuleMigrateStart (490) - The policy engine has started migrating files for a particular file-placement rule, identified in the trap. Use the place-rule command to create a file-placement rule.

policyRuleMigrateSuspend (494) - A placement rule has suspended its file migrations due to a schedule setting. The rule is identified in the trap text. Use the schedule command to create or edit a schedule, and use the duration command to set a time limit on the rule. Suspension happens when the duration expires before the rule has finished its processing.

A rule can also be suspended when policy is paused in its volume. You can use policy pause (gbl-ns-vol) to pause a volume's rules on a scheduled basis, or policy pause to pause all of a volume's rules immediately.

policyRuleMigrateResume (495) - The policy engine has resumed migrating files for a particular file-placement rule, identified in the trap.

policyRuleMigrateComplete (500) - The policy engine has completed migrating files for a particular file-placement rule, identified in the trap.

The Running State for a File-Placement Rule

policyRuleRunStart (520) - An administrator has enabled a file-placement rule, or the rule's schedule has started a new run. The rule is identified in the trap text.

policyRuleRunSuspend (522) - A rule's schedule has suspended it. The rule is identified in the trap text. Use the schedule command to create or edit a schedule, and use the duration command to set a time limit on the rule. Suspension happens when the duration expires before the rule has finished its processing.

A rule can also be suspended when policy is paused in its volume. You can use policy pause (gbl-ns-vol) to pause a volume's rules on a scheduled basis, or policy pause to pause all of a volume's rules immediately.

policyRuleRunResume (515) - A rule has resumed after having been suspended (see above). The rule is identified in the trap text.

policyRuleRunComplete (510) - A rule (identified in the trap text) has finished one run.

Miscellaneous Policy Traps

policyRuleShareFreeSpaceThresholdRaise (527) - This applies to a share that is the target of a file migration (for example, a file migration from a place-rule). The share has filled up enough to potentially drop below its free-space "maintain" threshold; a file migration failed because the file was large enough to exceed the threshold. You set this free-space threshold with the policy freespace command.

You can clear this alarm condition by migrating files off of the share with a new place-rule, or by changing the current place-rule to use different target share or share-farm (with more free space).

policyRuleShareFreeSpaceThresholdClear (526) - This applies to a share that is the target of a file migration (typically from a place-rule). The share has regained enough free space to go above its "resume" threshold, set by the policy freespace command.   The system also sends this trap when a new command resets the "resume" threshold so that it is lower than the current free space. This clears the condition heralded by an earlier policyRuleShareFreeSpaceThresholdRaise trap.

policyShareFarmFreeSpaceThresholdRaise (536) - This applies to a share farm that is the target of a file migration (typically from a place-rule). Every share in the share farm share has filled up enough to drop below its free-space "maintain" threshold, so the file cannot migrate to the share farm. (You set the free-space "maintain" threshold on each share with the policy freespace command.)

You can clear this alarm condition by adding one or more shares with available free space to the share farm (with share (gbl-ns-vol-sfarm)), or by changing the target of the place-rule.

policyShareFarmFreeSpaceThresholdClear (535) - This applies to a share farm that is the target of a file migration. At least one of the shares in the share farm has regained enough free space to go above its minimum “resume” threshold, so migrations to the share farm can continue. The resume threshold is set for each share with the policy freespace command.

This clears the condition heralded by an earlier policyShareFarmFreeSpaceThresholdRaise trap.

policyRuleShareFrequencyZeroRaise (529) - The share identified in the trap is no longer a target for new-file placement. This may mean that the share has reached its minimum free-space threshold, set with the policy freespace command. This trap also occurs when the share goes offline.

policyRuleShareFrequencyZeroClear (528) - The share identified in the trap is reinstated as a target for new-file placement. This clears the condition heralded by an earlier policyRuleShareFrequencyZeroRaise trap.

policyRuleShareMigrateLimit (525) - A placement rule reached the migration limit set with the limit-migrate command. There is at least one more file to migrate, which would have exceeded the limit.

policyRuleSourceUnavailable (533) - A place-rule cannot run because its source share (or its underlying volume) is unavailable. Use the from (gbl-ns-vol-plc) command to set the source for the rule.

policyRuleTargetFull (531) - A place-rule cannot run because its target share or volume is full. Use the target command to change the target for the rule.

policyRuleTargetUnavailable (532) - A place-rule cannot run because its target share or volume is unavailable. Use the target command to change the target for the rule.

policyRuleWarning (530) - This is a warning of a recoverable error condition, described in the trap text.

Volume-Scan Status

policyRuleVolumeScanStart (485) - A rule has started tree-walking a volume’s shares. This scan is an important phase in copying or migrating files. This applies to any type of rule except the shadow-copy rule: place-rule, auto-migrate, or balance.

policyRuleVolumeScanSuspend (483) - A rule’s schedule has suspended it in the middle of its volume-scanning phase. The rule is identified in the trap text. Use the schedule command to create or edit a schedule, and use the duration command to set a time limit on the rule. Suspension happens when the duration expires before the rule has finished its processing.

A rule can also be suspended when policy is paused in its volume. You can use policy pause (gbl-ns-vol) to pause a volume’s rules on a scheduled basis, or policy pause to pause all of a volume’s rules immediately.

policyRuleVolumeScanResume (484) - A place-rule, auto-migrate, or balance rule has resumed a tree-walk after pausing. The pause is caused by the duration in the rule's schedule. The scan resumes where the previous run left off.

policyRuleVolumeScanComplete (480) - A place-rule, auto-migrate rule, or balance rule has successfully tree-walked a volume's shares.

Power

You can add either of these traps to an email event (see email-event). They are part of the "chassis" event group.

powerFail (540) - A power supply (identified in the trap) has failed. On an ARX-1500, ARX-2000, ARX-2500, or ARX-4000, you can contact F5 Support to get a replacement power supply. The smaller platforms do not have replaceable power supplies and must be entirely replaced. Their Hardware Installation manuals contain ARX-replacement procedures.

powerStatus (542) - This indicates a change in power status, either on the chassis level or the module level. A chassis-level trap indicates that "PowerA" or "PowerB" is supplying power to the chassis. A module-level trap shows that the status changed to "on line" from a failure state.

Pre-Win2K Name Mismatches

Some Windows Domains existed before Windows 2000 was released, and supported 15-byte NetBIOS names for their domains (for example, "MYDOMAIN"). Fully-qualified domain names (FQDNs), such as "domain.company.com," are used today. Many domains have an FQDN that is an extension of the former NetBIOS name: for example, "MYDOMAIN" could have become "mydomain.mycompany.com." In some cases, the old-style NetBIOS name is completely different from the FQDN: suppose, for example, that "YOURDOMAIN" became "anotherdom.yourco.com."

The ARX can automatically discover the NetBIOS names from your Active Directory (AD), or you can set them manually on the ARX. These traps are for cases where a set name does not match the discovered name.

You can configure these traps as email events (see email-event). They are part of the "chassis" event group.

prewin2kMismatchRaise (546) - The Windows AD keeps records of old-style domain names for each FQDN, and the ARX can automatically discover those old-style names. You can also set the old-style domain name in any of the following CLI operations (or their GUI equivalents):

- windows-domain (gbl-proxy-user),
- windows-domain (gbl-gs),
- user (gbl-mgmt-auth), or
- windows-domain (gbl-ntlm-auth-srv).

The ARX raises this trap when one of the above names is set by an ARX administrator to something different than the name discovered at the AD. The trap text identifies the configuration object with the mismatched name.

In most cases, the discovered name is correct. You can accept the discovered name by running one of the commands above without any **pre-win2k** option. If you change the name at a domain controller, you can use the active-directory update forest command to discover the new name.

prewin2kMismatchClear (547) - A formerly mismatched pre-Windows 2000 name now matches. Either the name changed at the external AD or at the ARX. This clears the alarm condition raised by the ‘prewin2kMismatchRaise’ trap.

RAM Errors

You can configure these traps as email events (see email-event). They are part of the “chassis” event group.

ramECCCorrectableError (551) - The Error-Check Circuitry (ECC) found write errors in Random Access Memory (RAM) for one of the processors. The internal firmware corrected the errors immediately, so the trap is informational. If you see many of these errors, contact F5 Support; there may be an underlying hardware issue.

ramECCError (550) - The Error-Check Circuitry (ECC) found write errors in Random Access Memory (RAM) for one of the processors. The internal firmware was unable to correct the error. Contact F5 Support if you see this trap.

In extreme cases, this can lead to a processor failure. In a redundant pair, this may cause a failover to the peer chassis. On an ARX-4000, you can replace the module with the failed CPU (indicated in the trap); on the smaller, less-modular platforms, you must replace the entire ARX and return the failed unit to the factory. Use the instructions in the appropriate Hardware Installation manual to replace the module or the ARX.

ramMissingRaise (552) - A Random Access Memory (RAM) module is no-longer detectable on the ARX chassis. The chassis software has less RAM available than the amount that was configured at the factory. This may indicate that a memory module has come loose or has failed. The ARX must be powered down to re-seat or replace a memory module: contact F5 Support to perform this procedure.

There is no corresponding “clear” trap for this alarm condition. When the chassis powers back up, the chassis software checks for sufficient memory and only raises the alarm if memory is still missing.

systemBusError (733) - The CPU received an error from the system bus, a data pipeline between a CPU and other hardware components. Contact F5 Support if you see this trap.

RAID

These traps concern the internal disks on the ARX, where configuration files, logs, reports, and other administrative data are stored in a RAID. You can configure these traps as an email events (see email-event). They are part of the “chassis” event group.

raidVerifyRaise (548) - The raid verification-mode command is set to manual, and the RAID verification process has not run for at least 24 hours. We strongly recommend running RAID verifications at least once each day. To clear this alarm condition immediately, use the raid verify command. Use the raid verification-mode automatic CLI command to run RAID verifications regularly and avoid future occurrences of this trap.

raidVerifyClear (549) - The RAID verification process has run and cleared the alarm condition raised by “raidVerifyRaise.” The RAID verification process runs when someone invokes the raid verify command, or when the ARX automatically starts it because raid verification-mode automatic is set.

Reserve-File Limits

reserveFileLimitRaise (554) - A volume has used 75% of its file credits. A volume requires one *file credit* for each of its files and directories. Clients cannot add any more files or directories after all of the volume’s file credits are used. This trap can have one of two meanings, depending on the volume’s setting for the auto reserve files command.

If auto reserve files is disabled, the volume is approaching its maximum *files*. That is, the number of used files is approaching the volume’s assigned file credits. You can use the reserve files command to manually raise the volume’s file credits, or you can use the auto reserve files command to allow the volume to automatically raise its file credits as needed. If the number of file credits is currently near the maximum, too, start planning for a volume split or migration. Contact F5 Support for help with splitting a volume or migrating it to a new volume-group.

If auto reserve files is enabled, the volume is approaching its maximum file *credits*. The volume automatically reserves more file credits whenever its available file credits run low. Either the volume or its volume group is gradually approaching its limit; you can use show namespace to see the volume’s file credits and show volume-group to see the file credits in the volume’s group. Then contact F5 Support to start planning to split the volume or move it to another group.

You can configure this trap as an email event (see email-event). It is part of the “storage” event group.

reserveFileLimitClear (555) - A volume that previously was above 75% utilization of its file credits has fallen below 75%. This indicates one of two conditions, depending on the volumes auto reserve files setting:

- If auto reserve files is disabled, the maximum number of *files* has increased. This indicates that someone increased the number of file credits in the volume, either with the reserve files command or its GUI equivalent.
- If auto reserve files is enabled, the maximum number of file *credits* has increased. This is only possible if some other volume was removed from the volume's group, therefore increasing the available file credits for all remaining volumes in the same group.

You can configure this trap as an email event (see email-event). It is part of the "storage" event group.

reserveFileLimitCancel (556) - A volume that previously was above 75% utilization of its file credits has been removed. (You can use the remove namespace namespace volume vol-path command to remove a volume.) You can safely ignore any previous reserveFileLimitRaise trap for this volume.

You can configure this trap as an email event (see email-event). It is part of the "storage" event group.

reserveFileIncrease (557) - A volume's file credits have automatically increased. This indicates that the volume has auto reserve files enabled, and that its number of files and directories was approaching its former file-credit limit. Now the volume can hold more files and directories.

Resource Failures, Non-Critical

You can configure these traps as an email events (see email-event). They are part of the "chassis" event group.

resourceFailureRaise (560) - A process failed. This failure is not critical to the system, so it does not cause a reboot or failover. The failed process is identified in the trap text.

resourceFailureClear (561) - A previously-failed process has recovered.

Restore

restoreDataStart (574) - Someone has started restoring a volume's files and directories through a VIP. You can use the restore data command to start a restore operation from the CLI.

restoreDataComplete (572) - The ARX has finished restoring a volume's files and directories. The restore operation was successful.

restoreDataCanceled (571) - An administrator has canceled the given restore operation. The CLI command, cancel restore data, can cancel a restore operation.

restoreDataFail (573) - A restore operation failed. The namespace name, volume name, and path of the restore operation are shown in the trap data.

RON

ronTunnelState (576) - The RON tunnel identified in the trap has changed state. The state change is specified in the trap. For a list of possible tunnel states, see the CLI-reference documentation for show ron tunnel.

SAM Reference Filer

You can configure either of these traps as an email event (see email-event). They are part of the “storage” event group.

samReferenceOfflineRaise (972) - A namespace’s SAM-reference filer has gone offline. The IP address of the SAM-reference filer is in the trap, along with the namespace that is affected by this issue. The namespace’s CIFS clients cannot access any of its local-group names without this filer reference. Use the ping, expect traceroute, and show exports commands to verify connectivity between the SAM-reference filer and the ARX. If necessary, go to the filer and restart services, or use the sam-reference command to choose another SAM-reference filer.

samReferenceOfflineClear (973) - A namespace’s SAM-reference filer has come back online. This clears the alarm condition raised by the samReferenceOfflineRaise trap.

Secure Agent

secureAgent (580) - reserved for future use.

Service Issues

These traps pertain to front-end cifs or nfs services that are being analyzed by the stats-monitor process. The *stats-monitor* process analyzes round-trip time (RTT) statistics and error counts between the ARX services and their clients, as well as some internal statistics. It keeps a moving average of these statistics and raises a trap if they suddenly rise too far above the average for too long.

You can add any of these traps to an email event (see email-event). They are part of the “statsmon” event group.

serviceErrorsRaise (586) - The stats-monitor process has detected that a front-end service has suddenly started receiving a large number of errors from its clients. The service name (typically its FQDN) and virtual-IP address (VIP) are both identified in the trap text. The stats monitor counts errors from all clients, and this trap appears if the error counts increase significantly from their moving average, and if the increase persists over some number of samples. You can use the moving-average command to set two thresholds for this trap: the percentage increase that is significant enough to merit a trap, and the number of samples that are required.

This trap never appears unless you enable stats-monitor traps with the trap command. To enable stats-monitor traps for NFS services, use notify nfs-service followed by trap. To enable stats-monitor traps for CIFS services, use notify cifs-service followed by trap.

serviceErrorsClear (587) - A cifs or nfs service that was formerly receiving a higher-than-average number of errors has returned to an error count that is not significantly above the moving average. The service is identified in the trap text. This may indicate that the service's number of errors has decreased, or it may indicate that the increased error count has remained steady for a large number of samples, or a combination of the two. In any case, the error counts have been fairly consistent over a large number of samples. For some number of error-count samples, the error count has not been significant enough to merit an alarm, as determined by the settings of the moving-average command.

This clears the alarm that was formerly raised by a 'serviceErrorsRaise' trap.

As with the serviceErrorsRaise trap, this trap never appears unless you enable stats-monitor traps with the trap command. To enable stats-monitor traps for NFS services, use notify nfs-service followed by trap. To enable stats-monitor traps for CIFS services, use notify cifs-service followed by trap.

serviceSlowRaise (578) - The stats-monitor process has detected that a front-end service has suddenly slowed. The service name (typically its FQDN) and virtual-IP address (VIP) are both identified in the trap text. Round-trip times (RTTs) are measured for all communication between the service and its clients, and this trap appears if the times increase significantly from their moving average, and if the increase persists over some number of RTT samples. You can use the moving-average command to set two thresholds for this trap: the percentage increase that is significant enough to merit a trap, and the number of RTT samples that are required.

This trap never appears unless you enable stats-monitor traps with the trap command. To enable stats-monitor traps for NFS services, use notify nfs-service followed by trap. To enable stats-monitor traps for CIFS services, use notify cifs-service followed by trap.

serviceSlowClear (579) - A front-end service that was formerly slow has returned to a round-trip time (RTT) that is not significantly above the moving average. The service is identified in the trap text. This may indicate that the service's RTT time has decreased, or it may indicate that the increased RTT has remained steady for a large number of samples, or a combination of the two. In any case, the RTTs have been fairly consistent over a large number of samples. For some number of RTT samples, the RTT has not been significant enough to merit an alarm, as determined by the settings of the moving-average command.

This clears the alarm that was formerly raised by a 'serviceSlowRaise' trap.

As with the serviceSlowRaise trap, this trap never appears unless you enable stats-monitor traps with the trap command. To enable stats-monitor traps for NFS services, use notify nfs-service followed by trap. To enable stats-monitor traps for CIFS services, use notify cifs-service followed by trap.

Service Rejoin (CIFS)

You can configure these traps as an email events (see email-event). They are part of the “cifs” event group.

serviceRejoinRequiredRaise (581) - The first part of a CIFS service’s FQDN is longer than 15 bytes, so you must rejoin it to its Windows domain. The first part of the FQDN is the part before the first period (.); for example, “athos” in “athos.musketeers.gov.” The CIFS service’s FQDN appears in the trap. The CIFS service was evidently joined to the domain with an earlier release of software, when longer names were permitted. To rejoin the service to the domain, rerun the domain-join command.

serviceRejoinRequiredClear (582) - A CIFS service has rejoined its Windows domain, thereby clearing the alarm condition raised by the serviceRejoinRequiredRaise trap. The rejoined service is identified in the trap.

This may also indicate that the CIFS service is starting (perhaps with a no enable (gbl-cifs, gbl-nfs)/enable), and is clearing the alarm condition before it checks for the issue. In this case, it is possible for the service to re-discover the problem and issue a subsequent serviceRejoinRequiredRaise trap.

Shadow Copy

shadowTargetFail (600) - A shadow-copy operation has failed for a given shadow-volume target (target (gbl-ns-vol-shdwcp)), shown in the trap.

shadowCopyFail (590) - All targets failed for shadow-copy operation. Each target sent a shadowTargetFail trap, described above. The shadow-copy-rule command creates a shadow-copy rule.

shadowMetaDataShareFreeSpaceWarnRaise (606) - The metadata share at the rule’s target (gbl-ns-vol-shdwcp) volume is low on free space. For some installations, the target volume’s metadata share holds an important database for the shadow-copy rule; the database-location command determines the database location for the rule. If the target volume holds the shadow-copy database (as is recommended), the database is in danger of running out of space. The available free space and the free-space threshold are included in the trap. Access the target volume’s metadata share directly and clear some space, or use nsck ... migrate-metadata to migrate the target volume’s metadata to a larger share. At the target volume’s ARX, you can use show namespace to find the metadata share that the target volume uses.

This trap comes from the shadow-copy rule's source volume. The target volume may also send a separate 'metaDataFreeSpaceThresholdRaise' trap.

You can configure this trap as an email event (see email-event). It is part of the "policy" event group.

shadowMetaDataShareFreeSpaceWarnClear (605) - The metadata share at the rule's target (gbl-ns-vol-shdwcp) volume now has ample free space. This clears the error condition from a previous 'shadowMetaDataShareFreeSpaceErrorRaise' trap.

This trap comes from the shadow-copy rule's source volume. The target volume may also send a separate 'metaDataFreeSpaceThresholdClear' trap.

You can configure this trap as an email event (see email-event). It is part of the "policy" event group.

shadowMetaDataShareFreeSpaceErrorRaise (608) - The metadata share at the rule's target (gbl-ns-vol-shdwcp) volume is very low on free space. The currently-available free space (included in the trap) is now lower than it was when the same volume sent an earlier 'shadowMetaDataShareFreeSpaceWarnRaise' trap. Access the target volume's metadata share directly and clear some space, or use nsck ... migrate-metadata to migrate the target volume's metadata to a larger share. At the target volume's ARX, you can use show namespace to find the metadata share that the target volume uses.

This trap comes from the shadow-copy rule's source volume. The target volume may also send a separate 'metaDataFreeSpaceThresholdRaise' trap.

You can configure this trap as an email event (see email-event). It is part of the "policy" event group.

shadowMetaDataShareFreeSpaceErrorClear (607) - The metadata share at the rule's target (gbl-ns-vol-shdwcp) volume now has adequate free space. This clears the error condition from a previous 'shadowMetaDataShareFreeSpaceErrorRaise' trap, though a warning (from shadowMetaDataShareFreeSpaceWarnRaise) may still be in effect.

This trap comes from the shadow-copy rule's source volume. The target volume may also send a separate 'metaDataFreeSpaceThresholdClear' trap.

You can configure this trap as an email event (see email-event). It is part of the "policy" event group.

Share Status

Free Space

shareFreeSpaceWarningRaise (622) - reserved for future use.

shareFreeSpaceWarningClear (621) - reserved for future use.

shareFreeSpaceThresholdRaise (620) - The share identified in the trap has fallen below 512 M of free space. If this is cause for concern and the volume is a managed volume, you can use a place-rule to migrate a set of files to another share in the same volume.

You can configure this trap as an email event (see email-event). It is part of the “storage” event group.

shareFreeSpaceThresholdClear (610) - The share identified in the trap has risen above 768 M of free space. This clears the alarm condition that was raised by an earlier ’shareFreeSpaceThresholdRaise’ trap.

You can configure this trap as an email event (see email-event). It is part of the “storage” event group.

Feature Mismatch Between Back-End Shares and ARX Configuration

You can configure either of these traps as email events (see email-event). They are part of the “storage” event group.

shareFeatureMismatchRaise (623) - An ARX volume records the “cifs.perserve_unix_security” setting from its back-end NetApp shares during import. This trap indicates that an administrator changed that feature setting after the share was imported. This inconsistency can cause file migrations and directory striping to fail. To correct this alarm condition, access the NetApp share directly and change the “cifs.perserve_unix_security” option back to its former setting. The NetApp IP address and share name are both included in the trap.

shareFeatureMismatchClear (624) - The NetApp share identified in the trap formerly had a mis-matched setting for its “cifs.perserve_unix_security” option, and now the mis-match has been corrected. The option is set the same way that it was during the import of the share. This clears the alarm condition raised by the shareFeatureMismatchRaise trap.

Import

shareImportStart (660) - A volume has started importing a share. This is invoked by enabling the namespace, volume, and share (with enable (gbl-ns, gbl-ns-vol) and enable (gbl-ns-vol-shr)).

shareImportComplete (630) - A volume has successfully imported a share.

You can configure this trap as an email event (see email-event). It is part of the “storage” event group.

shareImportDirScanComplete (640) - A volume has successfully tree-walked a share, a major phase in importing the share.

shareImportFail (650) - A share import has failed. The trap text describes the failure. The details of the failure appear in the share’s import report; use show reports to find and view the import report. For a list of possible import failures and documentation for resolving them, see the show namespace documentation.

You can configure the above trap as an email event (see email-event). It is part of the “storage” event group.

Login Failures at the Filer

shareLogonFailureRaise (666) - A namespace lost its privileges to access a CIFS back-end share. The back-end filer and share are identified in the trap. Check the back-end filer to verify that the namespace’s proxy-user has permissions to read and write to this share. The proxy-user credentials must belong to the Backup Operator’s group at this filer. Use show global-config namespace to find the proxy user assigned to a namespace, and use show proxy-user to see the Windows credentials associated with the proxy user.

You can configure this trap as an email event (see email-event). It is part of the “storage” event group.

shareLogonFailureClear (665) - A back-end share that was inaccessible earlier (as announced by a shareLogonFailureRaise trap) is now accessible.

You can configure this trap as an email event (see email-event). It is part of the “storage” event group.

Offline and Online

shareOffline (670) - A namespace share has gone offline: either the administrative status or the operational status has changed. An administrator can use no enable (gbl-ns-vol-shr) or no filer to change the share’s administrative status to “disabled.”

You can configure this trap as an email event (see email-event). It is part of the “storage” event group.

shareOnline (680) - A namespace share has come online. This means that both the administrative status and the operational status are positive. A user can change the share’s administrative status to “enabled” with enable (gbl-ns-vol-shr).

You can configure this trap as an email event (see email-event). It is part of the “storage” event group.

Share-Removal Traps

shareRemoveStart (710) - Someone started a share removal with no share, remove-share migrate, or remove-share nomigrate.

shareRemoveComplete (690) - A share has been successfully removed from its volume.

You can configure this trap as an email event (see email-event). It is part of the “storage” event group.

shareRemoveFail (700) - A share removal has failed. The remove commands (above) each generate a report that indicates the cause of the failure.

You can configure this trap as an email event (see email-event). It is part of the “storage” event group.

Share-Write-Access Traps

These traps alert you to a back-end filer that has denied write permission to the ARX. You can configure either or both of these traps as email events (see email-event). They are part of the “storage” event group.

shareWriteAccessFail (701) - A back-end filer denied write access to a managed volume. This may indicate that the volume’s proxy-user no longer has write permission at the filer, or it may indicate a more widespread issue for the filer or share. Check the filer directly for write-permissions issues; the filer and share are identified in the trap.

You can use show proxy-user to identify the CIFS-user account for the proxy user. Minimally, this user account requires write permission at the share. It should be a member of the Backup Operator’s group on the filer.

shareWriteAccessClear (702) - A filer that formerly blocked write access is now allowing writes. This clears the shareWriteAccessFail alarm, above.

Share-Ownership Traps

shareOwnershipStolen (711) - Another ARX has taken ownership of a running share in a managed volume. This means that all of the share’s files have vanished from client view. It is caused by a mis-use of the enable ... take-ownership CLI command (or its GUI equivalent); a managed volume should never take ownership of a back-end share that is being used by a running ARX. For correct use of this feature, refer to the documentation for enable (gbl-ns, gbl-ns-vol) or enable (gbl-ns-vol-shr).

shareTakeOwnership (712) - A managed volume has taken ownership of a share that was evidently owned by another ARX. This is a legitimate action in some cases. From the CLI, you can accomplish this with the take-ownership option in the enable (gbl-ns, gbl-ns-vol) or enable (gbl-ns-vol-shr) command.

shareOwnershipProbeFail (715) - The ARX continuously probes all of the shares behind its managed volumes to confirm that it still owns them. This probe triggers the shareOwnershipStolen trap if it finds that another ARX has taken the share. This trap indicates that the probe failed, perhaps due to a communication problem with the back-end filer(s). You can use show exports to check the network connection to the filer, and to check for other filer issues.

Filer-Probe Traps

shareRootSquashed (716) - The ARX discovered that an enabled back-end share has “root squash” enabled. The share is therefore unusable in the namespace.

shareTimeSkewRaise (718) - An enabled namespace share has a sizeable time skew, relative to the time on the ARX. The filer IP is included in the trap text. This skew can make Kerberos authentication impossible, and it can have an adverse affect on policy rules. We recommend using the same ntp server for the filer and the ARX.

You can configure the above trap as an email event (see email-event). It is part of the “storage” event group.

shareTimeSkewClear (717) - The time skew between the ARX and one of its filers has shrunk to an acceptable level. This clears the shareTimeSkewRaise alarm, above.

You can configure the above trap as an email event (see email-event). It is part of the “storage” event group.

shareWriteProbeFail (719) - The ARX tried and failed to write a test file on a back-end share. Check connectivity to the back-end filer, and verify that the *root* user (for NFS) and/or the proxy-user (for CIFS) has permissions to write to this share.

shareProbeUpgradeRaise (682) - The ARX was upgraded to a new release of software (using the boot system and reload operations), and the software for probing back-end shares has changed. The share in this trap was formerly tested with a now-outdated probe, so the latest probe is running against the share. The share is offline until the new probe is complete. The filer IP and share name are both included in the trap text. This trap should be cleared very soon with a shareProbeUpgradeClear trap; examine the share with show exports and/or probe exports if this alarm condition persists for a long time.

This share status is also reflected in the output for show namespace status.

You can configure the above trap as an email event (see email-event). It is part of the “storage” event group.

shareProbeUpgradeClear (681) - After a software upgrade, the ARX has successfully probed the share in the trap. The ARX used the new probe in the latest release of software. This clears the shareProbeUpgradeRaise alarm, above.

You can configure the above trap as an email event (see email-event). It is part of the “storage” event group.

Snapshots

You can add either of these traps to an email event (see email-event). They are part of the “snapshot” event group.

snapshotOpStart (584) - A volume has started creating a coordinated snapshot. A *snapshot* is a replica of all of the volume’s files and directories at a single point in time. The ARX volume coordinates snapshots by blocking client access to the volume and then invoking snapshot operations on each of its back-end filers. A snapshot rule defines the schedule for the volume's snapshots (if any) and the number of snapshots to retain. A snapshot operation begins whenever the rule's schedule fires, or if someone uses snapshot create to manually invoke the rule.

snapshotOpComplete (583) - A coordinated-snapshot operation has successfully completed.

snapshotOpFail (585) - A manual snapshot operation (snapshot create, snapshot verify, or snapshot remove) has failed. Any such operation creates a report with details about the failure. The reports are named "snap_*n_operation_date*.rpt," where

- *n* is an integer to identify the snapshot,
- *operation* is "create," "verify," or "remove," and
- *date* is the date and time that the operation ran.

From the CLI, you can use show reports type Snapshot to see a list of all available snapshot reports.

Spanning Tree

stpNewRoot (720) - The ARX has become the new root of the Spanning Tree. This is sent upon expiration of the Topology Change Timer immediately subsequent to the switch's election. Use spanning-tree to configure spanning-tree parameters on the ARX.

stpTopologyChange (730) - One of the ARX's ports changed from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. This trap is not sent if an stpNewRoot trap is sent for the same transition.

SPNs

You can add either of these traps to an email event (see email-event). They are part of the "network" event group.

spnAliasUpdateRaise (725) - An active-directory alias operation has failed for an ARX service. This command sets a Service-Principal Name (*SPN*) for the ARX service. To clear this alarm condition, check the connection to the DC as well as the operational status of the DC itself. The Windows domain and the ARX service's FQDN are included in the trap. You can use the show active-directory status command to find the active DCs that the ARX uses for the Windows domain.

spnAliasUpdateClear (726) - The active-directory alias operation succeeded for the first time since the 'spnAliasUpdateRaise' condition went into effect.

Subshares (CIFS Only)

These traps concern CIFS subshares. A *subshare* is any share within another, imported share. If a back-end subshare has a share-level ACL, the ARX must connect its clients directly to the subshare for the ACL to be enforced. By default, the ARX connects to the share that it imported from the filer, then descends to the subshare. To support subshare ACLs, you must configure the ARX to pass a client from a front-end subshare directly to its back-end equivalent. You use the filer-subshares command (or its GUI equivalent) to set up a managed volume for this subshare support, then you use export (gbl-cifs) ... filer-subshare to export a subshare to ARX clients.

You can add either of these traps to an email event (see email-event). They are part of the “storage” event group.

subshareExportDegradedRaise (728) - An administrator ran export (gbl-cifs) ... filer-subshare, sync subshares from-namespace, or sync subshares from-service to export one or more CIFS subshares, and subshare synchronization failed. *Subshare synchronization* is the process of discovering all back-end subshares behind a volume and replicating them (with their ACLs) on all of the volume’s shares. With one or more back-end subshares unsynchronized with the rest, clients of the front-end subshare cannot access some of its files. The front-end subshare is therefore “degraded.”

You can run show cifs-service *fqdn* for a list of all degraded subshares in the *fqdn* service. To get a report with details on this issue, you can run either of the above sync subshares commands with the optional tentative flag. Use the report to find and fix configuration issues at the filer or at the ARX. Then rerun sync subshares from-namespace or sync subshares from-service, without the tentative flag, to clear this alarm condition.

subshareExportDegradedClear (729) - A formerly-degraded subshare is now fully supported. This clears the alarm condition heralded by the ’subshareExportDegradedRaise’ trap.

Suspend Failover (redundancy)

You can add either of these traps to an email event (see email-event). They are part of the “redundancy” event group.

suspendFailoverRaise (731) - An administrator used suspend-failover to suspend all redundancy failovers for an ARX. While the ARX is in this state, it cannot failover to its peer. However, the ARX continues to log all conditions that would ordinarily cause a failover.

suspendFailoverClear (732) - An administrator re-instated failovers at an ARX where failovers were previously suspended.

Switch Reboot Required

switchRebootRequired (721) - The internal SNMP process stopped and restarted, leaving SNMP processing in an unreliable state. Please reload the ARX as soon as possible to correct this condition.

Sync Files

syncFilesStart (737) - An administrator started a metadata sync operation with the sync files command, or a sync operation started automatically in a volume with auto sync files enabled. Each sync operation generates a report that may indicate the cause of the failure. The trap text includes the namespace, volume, and path that is being synchronized.

syncFilesComplete (735) - The sync files operation completed successfully.

syncFilesCanceled (734) - The cancel sync command canceled a sync operation.

syncFilesFailed (736) - A sync operation failed. The trap text includes the namespace, volume, and pathname where the sync was attempted.

System Resources

You can add either of these traps to an email event (see email-event). They are part of the "chassis" event group.

systemResourceThresholdRaise (738) - An ARX processor or disk partition has exceeded a resource threshold. Either a processor is experiencing high CPU, memory, or swap-space usage, or one of the internal disk partitions is nearly full. The specific processor or disk partition is named in the trap, along with the resource type (CPU, memory, swap space, or disk space) and the threshold that has been exceeded.

For each resource type, the system may send a Warning trap, an Error trap, and/or a Critical trap. A processor sends an Error trap only after the Warning trap, and the Critical trap after the Error trap.

From the CLI, use show system tasks to see which software processes are running, and check show policy for new policy operations in progress. You can use show processors usage to view the history of CPU and memory usage. The show chassis diskuse command shows the current disk usage in every internal partition; you can use one of the move commands (such as move ... ftp, move ... {nfs|cifs}, or move ... scp) to move files off of a partition, or delete to remove them altogether.

Call F5 Support if you cannot find a reasonable explanation for the high resource usage.

systemResourceThresholdClear (739) - A processor resource (CPU, memory, or swap) or a disk partition has crossed back below a threshold. This clears the alarm condition announced by an earlier systemResourceThresholdRaise trap. The processor, resource type, and threshold are all identified in the trap.

Temperature Sensors

You can add either of these traps to an email event (see email-event). They are part of the “chassis” event group.

tempFail (740) - One of the temperature sensors crossed a minimum or maximum threshold for safe operation. Use the show chassis temperature command to see the exact temperature at all sensors in the ARX.

tempStatus (750) - The temperature status has changed to “normal” from a “too low” or “too high” state.

Virtual CIFS (CIFS Namespace and Front-End Service)

vcifsDirNotEmpty (785) - The namespace software detected files in a directory that, according to the metadata, should be empty. This is considered a metadata corruption. If the volume has auto sync files enabled, this causes the volume to start to re-synchronize its metadata with the actual contents of the filer(s) for that directory. If not, you can manually check and repair the namespace, volume, and path with the sync files command. For related information about this failure, use grep to search the syslog for messages with the string, “UNXNOTEMPTY.”

vcifsFilerTimeout (760) - A CIFS service (identified in the trap text) timed out in its attempt to contact a back-end filer. For more details, use grep to search the syslog for messages with the string, “DISPTMO.” You can use show exports to check the network connection to the filer, and to check for other filer issues.

vcifsNameCollision (765) - A CIFS filer reported an unexpected name collision when the managed volume tried to migrate a file or directory to it. The file or directory was not known (in the volume’s metadata) to be at that share. This indicates a metadata corruption, possibly caused by clients connecting directly to the back-end filer.

You can manually check and repair the namespace, volume, and path with the sync files command.

vcifsNetworkError (770) - A CIFS service’s dialog with a back-end filer was interrupted by a network error. For more details, use grep to search the syslog for messages with the strings, “DISPXMIT” or “DISPNORSP.” As stated above, you can use show exports to check the network connection to the filer.

vcifsSvcAcctRaise (775) - A CIFS service cannot get a Kerberos service ticket for itself, and therefore its CIFS clients cannot authenticate. Check the machine account for the CIFS service at one of its domain controllers (DCs). The trap includes the CIFS service's FQDN and the account name, along with the error message it received instead of a service ticket. You can use the show active-directory command to find all of the DCs that the ARX uses.

You can add this trap to an email event (see email-event), to be delivered through email as well as the standard SNMP-trap mechanism. It is part of the "cifs" event group.

vcifsSvcAcctClear (776) - A CIFS service that formerly could not get a service ticket for itself has successfully obtained a ticket. CIFS clients can now authenticate with the CIFS service. This clears the alarm condition raised by the vcifsSvcAcctRaise trap.

You can add this trap to an email event (see email-event), to be delivered through email as well as the standard SNMP-trap mechanism. It is part of the "cifs" event group.

vcifsNotFound (780) - The namespace software received a "file not found" error for a file that it has recorded in its metadata. This is considered a metadata corruption. If the volume has auto sync files enabled, this causes the volume to start to re-synchronize its metadata with the actual contents of the filer(s) for that directory. If not, you can manually check and repair the namespace, volume, and path with the sync files command. For related information about this failure, use grep to search the syslog for messages with the strings, "UNXNOTFOUND" or "UNXNOPATH."

vcifsNsmTimeout (790) - The connection from the ACM (where the namespace/server software runs) to the NSM timed out. Use the show chassis command to check the NSM's status. For related information about this failure, use grep to search the syslog for messages with "DISPTMOTEM."

vcifsSearchFail (795) - is not supported.

vcifsSearchNotFound (796) - is not supported.

vcifsTypeMismatch (800) - The CIFS service found a directory on the back-end filer that was thought to be a file, or a file that was thought to be a directory. Alternatively, the service tried to create a new file or directory, and found an existing object of the same name but the opposite type (for example, the service tried to create the file, "/var/log," and found a directory by that name was already in the filer share). In either case, the metadata for the file/directory is corrupted

If the volume has auto sync files enabled, this causes the volume to start to re-synchronize its metadata with the actual contents of the filer(s) for that directory/file. If not, you can manually check and repair the namespace, volume, and path with the sync files command. For related information about this failure, use grep to search the syslog for messages with the strings, "UNXOPENTYPE" or "UNXCRETYPE."

vcifsWorkJamRaise (806) - This indicates that more than half of a group of CIFS worker threads has been running for an abnormally long time. Each *worker thread* is a single process that performs one work item at a time from an internal *work list*. Each work list has a group of worker threads that services it. The message in the trap indicates the name of the work list, and the number of threads in the group. This slowness can be caused by a slow connection to a back-end filer or domain controller, or it may be an internal error. Use the ping, expect traceroute, and show exports commands to verify connectivity between back-end filers and the ARX. Contact F5 Support if this alarm condition persists and you cannot find any such cause for it.

You can add this trap to an email event (see email-event), to be delivered through email as well as the standard SNMP-trap mechanism. It is part of the "cifs" event group.

vcifsWorkJamClear (807) - All CIFS threads in a formerly slow worker-thread group are no longer slow. This clears the alarm condition raised by the vcifsWorkJamRaise trap.

You can add this trap to an email event (see email-event), to be delivered through email as well as the standard SNMP-trap mechanism. It is part of the "cifs" event group.

Virtual Servers

You can add any or all of these traps to an email event (see email-event), to be delivered through email as well as the standard SNMP-trap mechanism. They are part of the "virtual-server" event group.

virtualServerOffline (810) - A virtual server changed to "offline" status. This happens when an administrator issues a no enable (gbl-gs, gbl-gs-vs) for the virtual server itself or for its global server.

virtualServerOnline (820) - A virtual server changed from "offline" to "online" status. This happens when an administrator issues an enable (gbl-gs, gbl-gs-vs) for the virtual server itself or for its global server.

virtualServerRemove (821) - The specified virtual server was removed from its global server. A user can trigger this with no virtual server .

virtualServiceOffline (830) - A front-end service (for example, NFS or CIFS) went offline. A user can trigger this with a no enable (gbl-cifs, gbl-nfs) for the front-end service. You can use the show nfs-service or show cifs-service command for more details on the service state.

virtualServiceOnline (840) - A front-end service (for example, NFS or CIFS) came online after being offline. A user can trigger this with an enable (gbl-cifs, gbl-nfs) command for the front-end service.

virtualServiceRemove (841) - The named NFS or CIFS service was removed from global configuration. A user can trigger this with no cifs or no nfs.

NFS Access Control Lists

You can add either of these traps to an email event (see email-event). They are part of the “virtual-server” event group.

virtualServiceAclUpdateSuccess (827) - The given NFS export has complete, fully-resolved NFS access lists after a recent NIS update. You can use the nis update command to invoke a NIS update.

virtualServiceAclUpdateFail (826) - The NFS access list(s) for the given virtual service and export are incomplete. When NFS access lists use NIS netgroups, some hosts in the netgroup may not be resolvable, or the netgroup membership may grow beyond the limits of the access list. Consult the report from nis update for more detailed information.

VLANs

vlanDefaultCfgFailure (870) - reserved for future use.

vlanDeleteLast (860) - reserved for future use.

vlanRequestFail (850) - reserved for future use.

vlanRestoreFail (880) - reserved for future use.

Volumes

volumeDisable (920) - The volume named in the trap text was disabled. An administrator can use no enable (gbl-ns, gbl-ns-vol) or nsck ... destage to disable a volume.

volumeEnable (921) - The volume named in the trap text was enabled after previously being disabled. An administrator can use enable (gbl-ns, gbl-ns-vol) to enable a volume.

X2 Modules (10-Gigabit-Port Transceivers)

These traps apply to the transceivers on the ARX-2500 and ARX-4000. These transceivers are the connectors at each of the 10-Gigabit ports.

You can add either of these traps to an email event (see email-event). They are part of the “chassis” event group.

x2ModuleFail (970) - The X2 module identified in the trap has crossed a failure threshold. The port can no longer carry any traffic, or may fail soon.

x2ModuleClear (971) - A previously-failed X2 module (identified in the trap by its slot and port number) now has normal power and laser levels. This clears the alarm condition set by the x2ModuleFail trap.

phyUnsupportedRaise (985) - The ARX booted up with an unidentified transceiver module in one of its ports. This transceiver has not been fully qualified for operation with the ARX platform. We recommend contacting F5 Support to purchase a fully-qualified transceiver.

The ARX sends this trap every time it boots with an unidentified transceiver module. You can use the clear health phyUnsupportedRaise command to clear this alarm condition from the show health output. Until you replace the transceiver or load a new ARX release that supports it (with boot system and reload), the ARX re-issues this trap on every reboot.

phyUnsupportedClear (986) - An administrator used the clear health phyUnsupportedRaise command. This clears the alarm condition set by the phyUnsupportedRaise trap.

XIP (Proxy-IP) and Internal-IP Inconsistencies

You can add either of these traps to an email event (see email-event). They are part of the “chassis” event group.

xipLipInconsistencyRaise (974) - The ARX (or its redundant peer) has an inconsistency with its mapping of internal IP addresses, proxy-IP addresses, or NSM-core IDs. The specific issue, and the peer with the issue, is identified in the trap text. This issue is not serious unless, for some other reason, you intend to replace the peer with the inconsistency. Contact F5 Support if this alarm condition is raised for a peer you intend to replace.

xipLipInconsistencyClear (975) - The internal IP inconsistency above has been resolved. This clears the alarm raised by the xipLipInconsistencyRaise trap.

Contacting Customer Service

You can use the following methods to contact F5 Networks Customer Service:

F5 Networks Online Knowledge Base Online repository of answers to frequently-asked questions.	http://support.f5.com
F5 Networks Services Support Online Online customer support request system	https://websupport.f5.com
Telephone	Follow this link for a list of Support numbers: http://www.f5.com/training-support/customer-support/contact/