20- Software Management Configuration Commands

20.1 Software Management Configuration Command Tree

Description

This chapter gives an overview of nodes that are handled by "Software Management Configuration Commands".

Command Tree

----configure
----software-mngt
- sw-replacement-mode

----oswp
- **(index)**
- primary-file-server-id
- second-file-server-id

X download-set
X autofetch
- [no] activate
- [no] auto-verify
- [no] on-schedule-time

----database
- [no] activate
- [no] backup
- [no] backupv6
- [no] auto-backup-intvl

20.2 Software Replacement Mode Configuration Command

Command Description

This command allows the operator to change how the software is being replaced during OSWP activation.

User Level

The command can be accessed by operators with software management privileges, and executed by operators with software management privileges.

Command Syntax

The command has the following syntax:

> configure software-mngt sw-replacement-mode <SwMgnt::SwReplacementMode>

Command Parameters

Table 20.2-2 "Software Replacement Mode Configuration Command" Command Parameters

Parameter	Type	Description
sw-replacement-mode	Parameter type: <SwMgnt::SwReplacementMode> Format: (upgrade-via-active | upgrade-via-standby | lt-by-lt) Possible values: - upgrade-via-active : Selects mode to do software upgrade via active nt - upgrade-via-standby : Enables upgrade via Standby NT - lt-by-lt : Enables ISSU upgrade mode	*optional parameter* Defines the required mode for doing Software Replacement.

20.3 Software Management Overall Software Package Configuration Command

Introduction

The Overall Software Package (OSWP) can be in any one of the following states: operational, aborting, downloading, enabled, disabled, activated, and committed. The operator can perform such functions as download the OSWP or set of files, abort its download, or enable or disable its autofetch property. The operator can also specify primary and secondary TFTP-server IDs for downloading the database.

The operator can also configure the download set or the set of files that are needed before triggering activation.

Download a new OSWP

To download an OSWP, the system must have only one enabled/active/committed OSWP, the management channel between the system and the manager must be established, and the system must not be involved in another software download process.

The manager requests that the system download a new OSWP. The manager specifies the path name of the overall descriptor file, the TFTP-servers where the overall descriptor files are located, and the set of files the manager wants to have available on the system before activating the new OSWP.

The system downloads the overall descriptor files and stores them persistently. The system downloads the software files that are specified in the downloaded SWP descriptor files, on condition that sufficient resources are available for their persistent storage. The manager can monitor the progress of the download process with granularity.

The download process can be implicitly or explicitly interrupted. The implicit interruption can occur due to reasons such as the unavailability of enough resources to store SWP files, the system not being able to download or interpret the overall descriptor file, or the system not being able to download a selected SWP descriptor file. The explicit interruption can occur when the manager requests that the system abort the ongoing download process.

If there are no exceptions, the system has two OSWPs; the Enabled/Active/Committed OSWP and the new downloaded OSWP. The state of the new OSWP is Enabled/NotActive/UnCommitted.

If the system supports software load validation feature and auto-verify is configured for a downloading oswp, system will perform implicit digital verification of downloaded files.If the digital verification is success system will make the OSWP state as Enabled/NotActive/UnCommitted otherwise it is Disabled/NotActive/UnCommitted.Also it should be noted that If auto-verify enabled then download of feature not supported release will have limitation and will be made as disabled since it will not have Digital signature files to validate. In such cases operator has to disable auto-verify and download.

Finally, after a successful verification process, Operator has to manually cross verify the root-certificate displayed in CLI with the distributed root certificate via other channel for that package then only it is ensured that downloaded package not altered from its original source.

Abort an OSWP

The manager can abort an OSWP when the system has two OSWPs. The state of the first OSWP is Enabled/Active/Committed while the second OSWP is in one of the following three states: Enabled/NotActive/UnCommitted, Downloading/NotActive/UnCommitted, or Disabled/NotActive/UnCommitted. The management channel between the system and the manager is established and the system is not involved in any other software download process.

The manager requests that the system remove the NotActive/UnCommitted OSWP. The system removes all the persistent stored files and databases not related to the Enabled/Active/Committed OSWP. The state of the OSWP to be removed is Aborting/NotActive/UnCommitted during the complete removal operation.

After a successful abort, the system has only one OSWP. The state of this OSWP is Enabled/Active/Committed. Only files and databases related to this OSWP are stored persistently in the system.

Activate a Not-Active OSWP

To activate a not-active OSWP, the system requires two OSWPs. The state of one OSWP is Enabled/Active and the state of the second OSWP is Enabled/NotActive. The management channel between the system and the manager is established and the system is not involved in another software download process.

The manager requests that the system activates the Enabled/NotActive OSWP. In case the manager requests to activate with linked database, the system first selects an available database that is compatible with and linked to the Enabled/NotActive OSWP. In case the manager requests to activate with default database, the system creates a default database that is compatible with the Enabled/NotActive OSWP. The system then starts the activation process of the NotActive OSWP.

The activation can happen on active NT or on standby NT. Activation on standby NT is only possible in case the redundant NT board is equipped and hot standby and the NT board type supports it. In case the conditions to do the activation on standby NT are fulfilled, the system will select this option. In case these conditions are not fulfilled the system will select activation on active NT.

Finally, after the successful activation of the Not-active OSWP, the system has two OSWPs. The previous Not-active OSWP is now active, together with the selected compatible database. Also, the previous Active OSWP is still available, but NotActive. In case the activation was done on standby NT, the standby NT from before the activation will be the active NT after the activation.

Commit an OSWP

To commit an OSWP, the system requires two OSWPs. The state of the first OSWP is Enabled/Active/UnCommitted and the state of the second OSWP is Enabled/NotActive/Committed.

The manager requests that the system commit the active OSWP. The system removes all the persistent stored files and databases that do not belong to the Enabled/Active OSWP. The state of the OSWP to be committed is Enabled/Active/Committing during the complete commit operation.

Finally, after a successful commit process, the system has only one OSWP. The state of this OSWP is Enabled/Active/Committed. Only files related to this OSWP are stored persistently in the system.

Verify an OSWP

If the system supports software load validation feature Operator can perform explicit digital verification of an OSWP.To verify an OSWP, the availability state of the OSWP should be Enabled.

Finally, after a successful verification process, Operator has to manually cross verify the root-certificate displayed in CLI with the distributed root certificate via other channel for that package then only it is ensured that downloaded package not altered from its original source.

Abort Verify an OSWP

The manager can abort verify on an OSWP when the system running explicit verification on that OSWP.

Command Description

This command allows the operator to configure various OSWP attributes and parameters.

User Level

The command can be accessed by operators with software management privileges, and executed by operators with software management privileges.

Command Syntax

The command has the following syntax:

> configure software-mngt oswp (index) [primary-file-server-id <SwMngt::serverIdv6>] [second-file-server-id <SwMngt::serverIdv6>] [download-set <SwMngt::downloadSet>] [autofetch <SwMngt::autoFetch>] [no activate | activate <SwMngt::OswpAutoAct>] [no auto-verify | auto-verify <SwMngt::OswpAutoVerify>] [no on-schedule-time | on-schedule-time <Sys::TimeIOInMinsRef1970>]

Command Parameters

Table 20.3-1 "Software Management Overall Software Package Configuration Command" Resource Parameters

Resource Identifier	Type	Description
(index)	Format: - id of one of the two oswps - range: [1...2]	index to the swm oswp table

Table 20.3-2 "Software Management Overall Software Package Configuration Command" Command Parameters

Parameter	Type	Description
primary-file-server-id	Parameter type: <SwMngt::serverIdv6> Format: (<Ip::V4Address> | ipv6 : <Ip::InetAddressType>) Possible values: - ipv6 : Ipv6 address (only for management IPv6 supported boards) Field type <Ip::V4Address> - IPv4-address Field type <Ip::InetAddressType> - IPv6 address	*optional parameter* tftp/sftp server address for overall descriptor file
second-file-server-id	Parameter type: <SwMngt::serverIdv6> Format: (<Ip::V4Address> | ipv6 : <Ip::InetAddressType>) Possible values: - ipv6 : Ipv6 address (only for management IPv6 supported boards) Field type <Ip::V4Address> - IPv4-address Field type <Ip::InetAddressType> - IPv6 address	*optional parameter* 2nd tftp/sftp server address for overall descriptor file
download-set	Parameter type: <SwMngt::downloadSet> Format: (min-set | actual-set | complete-set)	*obsolete parameter that will be ignored* set of files needed before triggering activation

Parameter	Type	Description
	Possible values: - min-set : minimum set of files needed to activate - actual-set : files applicable for the board types - complete-set : all the files	
autofetch	Parameter type: <SwMngt::autoFetch> Format: disabled Possible values: - disabled : disable autofetch feature	*obsolete parameter that will be ignored* disable autofetch feature
[no] activate	Parameter type: <SwMngt::OswpAutoAct> Format: (manually | after-download | on-schedule) Possible values: - manually : manually activate the OSWP - after-download : enable the automatic activation of OSWP after downloading - on-schedule : enable the automatic activation of OSWP at the time defined in on-schedule-time	*optional parameter with default value: "manually"* determines when to active an OSWP
[no] auto-verify	Parameter type: <SwMngt::OswpAutoVerify> Format: (disabled | enabled) Possible values: - disabled : manually verify the OSWP - enabled : enable the automatic verification of OSWP after downloading	*optional parameter with default value: "disabled"* determines auto-verify of an OSWP after downloading
[no] on-schedule-time	Parameter type: <Sys::TimeIOInMinsRef1970> Format: - the time (yyyy-mm-dd:hour:minutes)	*optional parameter with default value: "1970-01-01 : 00 : 00"* the expected activation time of OSWP, range:[1970-01-01 00:00,2035-12-31 23:59]

20.4 Database Automatic Activation Configure Command

Command Description

This command configure database automatic activation and automatic backup states and attributes.

User Level

The command can be accessed by operators with software management privileges, and executed by operators with software management privileges.

Command Syntax

The command has the following syntax:

> configure software-mngt database [no activate | activate <SwMngt::DbAutoAct>] [no backup | backup <SwMngt::DbAutoBackup>] [no backupv6 | backupv6 <SwMngt::V6DbAutoBackup>] [no auto-backup-intvl | auto-backup-intvl <SwMngt::DbAutoBackIntvl>]

Command Parameters

Table 20.4-2 "Database Automatic Activation Configure Command" Command Parameters

Parameter	Type	Description
[no] activate	Parameter type: <SwMngt::DbAutoAct> Format: (after-download | manually) Possible values: - after-download : enable the automatic activation of database after downloading - manually : manually activate the OSWP	*optional parameter with default value: "manually"* determines when to active database
[no] backup	Parameter type: <SwMngt::DbAutoBackup> Format: (manually | activate : <Ip::V4Address> : <SwMngt::dbpath>) Possible values: - manually : manually backup of the database - activate : automatic backup of the database Field type <Ip::V4Address> - IPv4-address Field type <SwMngt::dbpath> - path for the db (example: /path_to_db) - range: [a-zA-Z0-9-_./] - length: x<=255	*optional parameter with default value: "manually"* backup destination of database
[no] backupv6	Parameter type: <SwMngt::V6DbAutoBackup> Format:	*optional parameter with default value: "manually"*

Parameter	Type	Description
	(manually | activate : <Ip::InetAddressType> / <SwMngt::dbpath>) Possible values: - manually : manually backup of the database - activate : automatic backup of the database Field type <Ip::InetAddressType> - IPv6 address Field type <SwMngt::dbpath> - path for the db (example: /path_to_db) - range: [a-zA-Z0-9-_./] - length: x<=255	IPv6 backup destination of database
[no] auto-backup-intvl	Parameter type: <SwMngt::DbAutoBackIntvl> Format: - the interval period for automatic backup - unit: hours - range: [1...168]	*optional parameter with default value: 24* the interval period for automatic backup