

# HPE Intelligent Network Server Release Notes

Release 09.01.30



**Hewlett Packard**  
Enterprise

# Notices

---

## Legal notice

© Copyright 2020 Hewlett Packard Enterprise Development LP

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

Printed in the US

## Trademarks

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Microsoft®, Internet Explorer is either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

© 2020 Google Inc. All rights reserved. Chrome™ is a trademark of Google Inc.

Apache Kafka, Kafka, and the Kafka logo are either registered trademarks or trademarks of The Apache Software Foundation in the United States and other countries.

# Contents

Notices .....	1
Preface .....	6
About this guide.....	6
Audience .....	6
Document history .....	6
Chapter 1 Introduction .....	7
1.1 Certified base release .....	7
1.2 Supported operating systems.....	7
1.3 Pre-requisite .....	7
1.4 Co-requisite software .....	7
1.4.1 iTP webserver/iTP secure webserver .....	7
1.4.1.1 INS CLIM and host installation software .....	8
1.4.2 CLIM OS .....	8
1.4.3 HPE NonStop system console installer.....	9
1.4.4 Browser.....	9
1.4.5 Oracle Java runtime environment and security warning .....	9
1.5 Open source software packaged with INS.....	10
1.6 Migration path.....	10
1.7 Support of HPE INS deployment on virtual Non-Stop using VNF Manager (CIS) in NFV environment .....	11
1.7.1 Verifying code signing on vINS RPM.....	11
1.8 Release highlights .....	12
1.9 Customer documentation.....	13
Chapter 2 New features.....	14
Chapter 3 New and changed information .....	15
3.1 Special notes.....	15
Chapter 4 Cases addressed in this release .....	17
4.1 SFDC Cases addressed .....	17
Chapter 5 Known limitations .....	18
5.1 Multiple SIP services defined under a single CLIM container process .....	18
5.2 Excessive CPU use by OSS application during idle periods.....	18
5.3 Diameter service activation limitation .....	18
5.4 File code 100 object files are not supported .....	19
5.5 Limitation on number of processes to be run .....	19
Chapter 6 Known issues.....	20
6.1 Front-back node configuration migration is not working during node installation .....	20
6.2 Accessing CCMI using HTTP URL, when CCMI is configured to run on HTTPS causes log file to be filled up.....	20
6.3 Remote operations on 64-BIT protect contexts are not functioning properly.....	20
6.4 Diameter command code routing feature does not work as expected .....	20

6.5 Alarms in CCMI getting truncated when it is more than 3 lines.....	21
6.6 Fault management screen of UI pathway does not show the full EMS text from \SZLOG .....	21
Chapter 7 Installation instructions .....	22
7.1 Important notes for Installation .....	22
7.1.1 Process Input Parameter RTR-REPLY-SIZE .....	22
7.1.2 Setting the Value of Max Path Retrans .....	22
7.1.3 Process Input Parameter SEGMENT-SIZE .....	22
7.1.4 CLIM Parameter Settings for CLIM OS Version ABA or greater.....	23
7.1.4.1 New Kernel Parameter for SCTP: "net.sctp.addip_noauth_enable" .....	23
7.1.4.2 New Kernel Parameter for SCTP: "net.sctp.addr_scope_policy" .....	23
7.1.4.3 Kernel Parameter for SCTP: "net.sctp.auth_enable" .....	24
7.2 Installation considerations.....	25
7.2.1 Installing CLIM software .....	25
7.2.1.1 Identifying existing SIP package .....	25
7.2.1.2 Removing existing INS SIP CLIM packages .....	25
7.2.1.3 Installing a new SIP package .....	26
7.3 Database information .....	26
7.4 Node installation instructions.....	27
7.5 Performing a backout .....	27

# List of tables

.....	
Table 1: Document history.....	6
Table 2: Supported operating systems .....	7
Table 3: INS CLIM and host installation software .....	8
Table 4: Minimum OS version for Gen10 hardware .....	8
Table 5: Minimum OS version for Gen9 hardware .....	8
Table 6: Minimum OS version for Gen8 and previous hardware versions .....	8
Table 7: Protocol libraries .....	8
Table 8: Browser .....	9
Table 9: Open source software .....	10
Table 10: SFDC Cases addressed .....	17

# List of figures

Figure 1: Java security warning ..... 9

# Preface

---

## About this guide

---

This document provides information on the HPE Intelligent Network Server (INS) 09.01.30 release.

## Audience

---

This document is targeting those personnel who require basic information about this release of the HPE INS product.

## Document history

---

Table 1: Document history

Date	Description
Oct 07, 2020	Finalized for Release 09.01.30 - General Availability.

# Chapter 1

## Introduction

---

The following is a release summary for HPE INS R09.01.30. This release is available on NB-Series, and NX-Series. HPE INS R09.01.30 is baselined on HPE INS R09.01.20 release which includes new features and defect corrections. For more information, see the [New Features](#) and [Cases addressed in this release](#) section.

### 1.1 Certified base release

---

HPE INS-R09.01.00

### 1.2 Supported operating systems

---

Table 2: Supported operating systems

NB-Series	Execute:	NSK	J06.22.00 or later
NX-Series	Execute:	NSK	L18.08.00 or later

### 1.3 Pre-requisite

---

The customer requires HPE NonStop SSL (T0910) with the following HPE NonStop security bundles to support HTTPS interface for HPE INS CCM1:

- PID QSN52/QSN51 on J-series
- BE014AC on L-series

### 1.4 Co-requisite software

---

#### 1.4.1 iTP webserver/iTP secure webserver

NB-Series

```
/usr/tandem/webserver/bin/httpd
Binder timestamp: 05JAN2011 19:26:44 LCT, 05JAN2011 13:56:44 GMT
Version procedure: T8996H03_21JAN11_ADV_H302_01
Version procedure: T8432H01_05MAY2006_CCPLMAIN
TNS/E Native Mode: runnable file
```

NX-Series

```
/usr/tandem/webserver/bin/httpd
Binder timestamp: 12NOV2014 13:00:36 LCT, 12NOV2014 07:30:36 GMT
Version procedure: T8432L01_01OCT2014_CCPXMAIN_01
Version procedure: T8997L01_18FEB15_BASE_L101_01
```



TNS/X Native Mode: runnable file

**NOTE:** This software is applicable only on NB-Series operating systems.

### 1.4.1.1 INS CLIM and host installation software

Table 3: INS CLIM and host installation software

CLIM	T8718H06^0991T08^IINS_R09_01_30
Host (NB Series)	T8718J06^1588T14^IINS_R09_01_30
Host (NX-Series)	T8718L18^1378T14^XINS_R09_01_30

### 1.4.2 CLIM OS

Table 4: Minimum OS version for Gen10 hardware

Operating system	Minimum supported version
NB-Series	T0853J03_01OCT2018_07SEP2018_CDX
NX-Series	T0853L03_01AUG2018_28AUG2018_DBF

Table 5: Minimum OS version for Gen9 hardware

Operating system	Minimum supported version
NB-Series	T0853J03_01OCT2018_07SEP2018_CDX
NX-Series	T0853L03_01AUG2018_28AUG2018_DBF

Table 6: Minimum OS version for Gen8 and previous hardware versions

Operating system	Minimum supported version
NB-Series	T0853H01_01OCT2018_07SEP2018_ADX
NX-Series	T0853L02_01AUG2018_22AUG2018_BBF

CLIM package IDs:

- ins-clim-m3ua-9.1.30
- ins-clim-sip-9.1.30
- ins-clim-diameter-9.1.30
- ins-clim-mon

Table 7: Protocol libraries

Library	Description	Version
Hpegmf	HPE Portability Generic Management Framework Library	1.1.1
Hpebus	HPE Portability Bus Library	1.1.1
Hpetbx	HPE Portability Toolbox Library	1.1.2
Hpesip	HPE SIP Stack libraries	1.1.3-150

## 1.4.3 HPE NonStop system console installer

DVD Product ID: S7X-SWV2/HNSC-SWV2/QNSC-SWV2, Update 22

## 1.4.4 Browser

Table 8: Browser

Browser	Tested version
Internet Explorer	11.0.9600.185371S
Google chrome	56.0.2924.87
Mozilla Firefox	51.0.1

## 1.4.5 Oracle Java runtime environment and security warning



**NOTE:** Following JRE version and security warning are applicable for the CCMI session invoked by html.

Version: 1.7.0\_25



**NOTE:** CCMI (HTML) does not support 64-bit JRE versions. It supports all the 32-bit JRE versions except 1.7.0\_71, 1.7.0\_72, and 1.8.0\_25.

When you access CCMI on the systems that are running certain Java versions, the following dialog box appears:

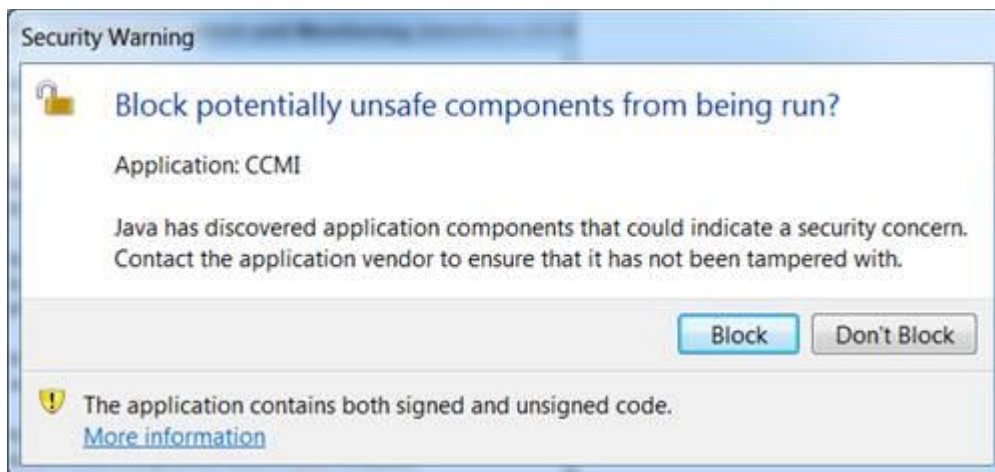


Figure 1: Java security warning

Click Don't Block to let the application continue the execution.

Alternatively, perform the following steps to prevent these security warnings:

1. In the Java Control Panel, click the Advanced tab.
2. Expand the Mixed code (Sandboxed Vs trusted) Security Verification option under the Security section.
3. Check Enable - hide warning and run with protections.

## 1.5 Open source software packaged with INS

---

The following table lists the open source software used by HPE INS:

Table 9: Open source software

Software	Version	Location
Boost	1.54.0	HPE CLIM software
Zulu JDK	10	HPE CCMI software
Inno setup	5.6.1	HPE CCMI software
jsonparser-C-language	1.0	HPE CCMI software
twbs-bootstrap-sass	2.3.2	HPE CCMI software
jdorn-json-editor	0.7.28	HPE CCMI software

## 1.6 Migration path

---

### IPM PAK file:

R07.00.xx → R09.01.00 → R09.01.20 → R09.01.30



**NOTE:** R07.00.xx indicates releases up to INS R07.00.14.

---

R07.01.xx → R09.01.00 → R09.01.20 → R09.01.30



**NOTE:** R07.01.xx indicates releases up to INS R07.01.32.

---

R08.00.xx → R09.01.00 → R09.01.20 → R09.01.30



**NOTE:** R08.00.xx indicates releases up to INS 08.00.13.

---

R08.01.xx → R09.01.00 → R09.01.20 → R09.01.30



**NOTE:** R08.01.xx indicates releases up to INS 08.01.32.

---

R08.02.xx → R09.01.00 → R09.01.20 → R09.01.30



**NOTE:** R08.02.xx indicates releases up to INS 08.02.05.

---

R09.00.xx → R09.01.00 → R09.01.20 → R09.01.30



**NOTE:** R09.00.xx indicates releases up to INS 09.00.02.

---

R09.01.xx → R09.01.20 → R09.01.30



**NOTE:** R09.01.xx indicates releases up to INS 09.01.10.

### Roll-up PAK file:

R09.01.00 → R09.01.30



**NOTE:** Ensure that you copy the correct installation PAK file to the target system.

Directory	PAK File	Description
NB-Series	INNB9100	INS base release 09.01.00
	INNI9130	INS IPM PAK file 09.01.30
	INNR9130	INS Roll up PAK file
NX-Series	INXB9100	INS base release 09.01.00
	INXI9130	INS IPM PAK file 09.01.30
	INXR9130	INS Roll up PAK file

The PAK file format is *INSTMmnn*, where:

- *S* is the system type and takes the following value:
  - *N* for NB-Series
  - *X* for NX-Series
- *T* is the release type and takes one of the following values:
  - *B* for a base release
  - *R* for a roll-up IPM
  - *I* for an incremental IPM
- *M* is the major release number
- *m* is the minor release number
- *nn* is the dot release number

## 1.7 Support of HPE INS deployment on virtual Non-Stop using VNF Manager (CIS) in NFV environment

### 1.7.1 Verifying code signing on vINS RPM

Before you begin

Make sure that the following prerequisite is met before verifying code signing:

- Code signing verification is being performed on the RHEL7.5 platform.

#### Procedure

**Step 1:** Login as root, execute.

**Step 2:** Create a directory where the HPE public keys will be stored

```
# mkdir -p signcheck
```

**Step 3:** Download the compressed HPE GPG Public Key.

```
# cd signcheck
```

```
# wget https://ftp.hp.com/pub/keys/HPE-GPG-Public-Keys.tar.gz
```

**Step 4:** Uncompress and extract the file content in sign check directory.

```
# gunzip HPE-GPG-Public-Keys.tar.gz
```

```
# tar xvf HPE-GPG-Public-Keys.tar
```

**Step 5:** We get a list of HPE Public Certificates and run the rpm import command to import the public certificate 2BAF2262.pub.

```
# rpm --import 2BAF2262.pub
```

**Step 6:** Verifying signature.

```
# rpm -Kv hpecms-vins-1.0.0-6864.el7.x86_64.rpm
hpecms-vins-1.0.0-6864.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature, key ID 2baf2262: OK
Header SHA1 digest: OK (7355c0f3bfe8c642421765fecf42b981901ba6c3)
V3 RSA/SHA256 Signature, key ID 2baf2262: OK
MD5 digest: OK (92dbdaeb39e23c40ce6288b2b1c2ab52)
```

For more information, see *HPE INS Installation Guide, Section 1.9 (Deploying HPE INS with CIS) and its sub-sections.*

## 1.8 Release highlights

---

This release includes new features and defect corrections. See the [New features](#) and [Cases addressed in this release](#) section for more information.

## 1.9 Customer documentation

---

The following customer documentation is available with this release. To view a summary of the changes made in a guide, open the guide and see the Preface > New and Changed Information section. This section includes links to new or modified information.

Document	Last update	Updated in this release?
Application Development Guide	R 09.01.30 / Oct 2020	Yes
C Application Programming Interface	R 09.01.30 / Oct 2020	Yes
CLI User's Guide	R 09.01.00 / Feb 2020	No
Configuration Planning Guide	R 09.01.30 / Oct 2020	Yes
Configuration Procedures Guide	R 09.01.30 / Oct 2020	Yes
JAVA API Guide	R 09.01.00 / Feb 2020	No
ERAD Database Utility User's Guide	R 09.01.00 / Feb 2020	No
Guide to ER Screening and Burst Control	R 09.01.00 / Feb 2020	No
Operations and Maintenance Guide	R 09.01.20 / Jul 2020	No
Guide to Statistics and CSRF Reporting	R 09.01.30 / Oct 2020	Yes
INS Glossary	R 09.01.00 / Feb 2020	No
INSCOM Utility User's Guide	R 09.01.00 / Feb 2020	No
Installation Guide	R 09.01.30 / Oct 2020	Yes
Introduction to HPE INS	R 09.01.30 / Oct 2020	Yes
Security Administration Guide	R 09.01.00 / Feb 2020	No
SNMP Customization Guide for the INS Platform	R 09.01.00 / Feb 2020	No
Mate to Mate Monitoring Utility User's Guide	R 09.01.00 / Feb 2020	No
HPE SIP Parser Application Development Guide	R 09.01.00 / Feb 2020	No
Open Source Software license information	R 09.01.30 / Oct 2020	Yes
INS Producer Interface Guide	R 09.01.30 / Oct 2020	Yes

# Chapter 2

## New features

---

**INS C API support for INS producer applications** - INS has implemented a few new C APIs, which have the capability to create topics, query metadata and send produce messages to topics of interest with acknowledgement enabled through APIs to a single Apache Kafka® cluster that has multiple brokers configured.

- The topic create API has additional parameters to provide partition numbers and replication factor while creating the topic.
- The produce message API has an additional parameter to specify the partition number to produce message to partition number of interest and acknowledgement parameter to choose the type of acknowledgement needed.
- The user can get cluster data information using the metadata query API.

**JSON tool to configure INS producer applications** - INS provides a JSON tool to insert and validate INS producer application configurations, which can be downloaded to a Windows system. This tool can also be used to create, modify and save the INS JSON file on the Windows system.

# Chapter 3

## New and changed information

---

### 3.1 Special notes

---

- To avoid NSDB errors: After upgrading a node from earlier release or migration of data from earlier release to the INS 09.00.00, “Input Queue Max” and “Output Queue Max” in ASUMMARY record must be manually updated appropriately. The default value is 7000.
- The length of the System Message Header (SMH) is increased, request to use the API, `L_GET_SMH_HDR_LENGTH` to get the exact length of SMH in bytes.
- CTX 32bit and PDBM SUPERVISOR PROCESS are no longer supported. So, the corresponding executables (CSSGNOBJ.CTXMME and CSSGNOBJ.PDBMSUE) and process description records (35 and 25) are not delivered as part of HPE INS 09.00.00. For nodes upgraded to HPE INS 09.00.00 a configuration change of setting Minimum Copies and Maximum Copies to 0 for PDESCs 35 and 25 is needed for the node to start successfully.
- Process input Parameters numbered 6 (XMEM-SEGMENT-TYPE), 8 (SEGMENT-SIZE), and 9 (CTX-SEGMENT-TYPE) are not in-use and not delivered from HPE INS 09.00.00. These PIPs can be removed or deleted, on upgraded nodes.
- Due to a new feature added to HPE INS Diameter in release INS 09.00.00, the size of the diameter session is increased. Applications must use C-API “`L_DIA_GET_SESSION_INFO_SIZE`” to know the exact size of the diameter session and then allocate enough memory to fetch the session information using API “`L_DIA_GET_SESSION_INFO`”.
- When CCMI is opened through CCMI Client launcher, the Online Help opens in the default browser of the system. The Contents, Index, Back, Forward and Exit functionalities of CCMI Online Help window are not available when CCMI is launched through the CCMI Client launcher.
- From INS 9.0 release onwards, opening a CCMI session of the node directly by using the URL <http://system-name/ss7/node-name/ccmi.html> is not supported.
- The PLIBRARY provided by INS will no longer be made available to the user as a usable library. All the configured PLIBRARY loaded customer applications should be replaced with NLIBRARY and all future applications should be compiled only with NLIBRARY.
- CTX 32-bit is no more supported. Only CTX 64-bit is supported from the release 08.01.00. Applications that are running on CTX 32-bit will now run seamlessly on CTX 64-bit. A configuration change is required, and the node will not start without PDESC records change. For more information about PDESC records, see [Update the number of copies of PDESC](#).
- Effective release 08.01.00, support for TE1, TE2, and TE3 link types have been removed.
- A new API, `L_GET_SMH_HDR_LENGTH` has been introduced. `L_GET_SMH_HDR_LENGTH` API returns the length of the System Message Header (SMH) in bytes.



- A Process Input Parameter `USE-DEF-CP-TASKID` is available. This Process Input Parameter must be used to provide the desired Call Processing Task ID to the non-call processing application process, using `L_GET_SSN API`, or `L_GET_SSN_TID API`. In such situations, the parameter `USE-DEF-CP-TASKID` must be added as `Param index` in the Process Description record, corresponding to the non-call processing process. A default value of standard call processing Task ID 40 is assumed, in the absence of an explicit value being set for this parameter, or when the parameter is not defined. For more details, see, *HPE INS Configuration Planning Guide*, and *HPE INS C Application Programming Interface Guide*.
- CCMI does not support 64-bit JRE versions. CCMI does not support 32-bit JRE versions 1.7.0\_71, 1.7.0\_72, and 1.8.0\_25. It supports all the other 32-bit JRE versions.
- The `ins-clim-mon` process of the earlier releases might not correctly monitor the processes of INS 07.00.10 or later.
- Alarm truncation in INS for `insAlarmActivateTrap`: In INS SNMP and alarm text in the `insAlarmActivateTrap` cannot exceed 12 lines of text. All the INS cross referenced ERADS will not have any duplicated texts. Instead, the first line of the cross referenced ERAD will be NSK subsystem name (subsystem number). event number, date and time, when the parameter `XREF-ERAD-DUP-TEXT` is set to N.
- Difference between the parameters `ENABLE-STATS-TRAP` and `ENABLE-STATS-COLLECTION`: `ENABLE-STATS-TRAP` will either enable or disable the statistical traps that are sent to the SNMP manager. The parameter `ENABLE-STATS-COLLECTION` either enables or disables the collected statistics.
- CCMI opens with JNLP support (CCMI.JNLP) from INS Version 08.01.10. Prior to this release, older way of using CCMI shall be applicable (CCMI.HTML).
- Default CCMI behavior changes to JNLP from INS Version 08.01.10.
- At minimum, JRE version 1.7 is required for JNLP support.
- CCMI with JNLP supports all the web browsers.
- MIGCFG enhancement: MIGCFG tool will not migrate configuration for INS-PDESC (Range 1 to 999) and PARAMS number 2032 from Front node.
- HPE INS 8.2 and above releases must have the COBOL native libraries (800 for J-series and 500 for L-series) to be licensed. Otherwise, certain operations on the HPE INS UI screen will be denied. When the NSK OS (J-series and L-series) does not include the Native Mode COBOL (NM COBOL) license (that is, if T0357 (for NB-series) and T0914 (for NX-series) is not listed in `SYSTEM.SYSnn.SWCONFIG`), this issue manifests on some of the HPE INS UI screens.

## Chapter 4

### Cases addressed in this release

---

The following section list the defects corrected in this release.

#### 4.1 SFDC Cases addressed

---

Table 10: SFDC Cases addressed

Sl. No.	SFDC Case ID	Title	Fix description	Severity
1	5348709006	SFDC 5348709006: Diameter services do not start on 9.1.11	The issue was caused as zero was being passed for initialization. The stack throws exception for zero entry. Removed the exception from stack for zero entry.	Minor
2	5348585235	SFDC 5348585235: Problems with NSDBCOMP	Corrected report footer and HPE branding.	Minor
3	5343819544	SFDC 5343819544 INS: Memory Manager abends on FSLEE app call attempt	Memory Manager does not abend anymore when LRC is configured	Minor
4	5349865606	SFDC 5349865606 Docs missed some stats groups reserved for INS	Documented the statistics group numbers used and reserved for INS.	Minor
5	5349361763	SFDC 5349361763 INS Installation fails	Added TMF information in Installation Guide	Minor

## Chapter 5

### Known limitations

---

#### 5.1 Multiple SIP services defined under a single CLIM container process

---

When configuring more than one SIP service on a CLIM, the "CLIM Protocol Service Port" for these services must be different. Otherwise, not all SIP statistics are reported correctly.

#### 5.2 Excessive CPU use by OSS application during idle periods

---

The OSS application can consume an excessive amount of CPU resources during idle periods. To mitigate this situation, you can define a process input parameter (PIP) in the OSS application's PDESC to allow configuration of a delay to prevent excess CPU use during idle periods. To define the PIP, perform the following steps:

1. Add a PIP to the OSS application's PDESC record using the procedure in the *Configuration Procedures Guide* with the following values:
  - Parameter Record: Any unused parameter record number
  - Parameter Name: MTS-OSS-DELAY
  - Text: The parameter's units are hundredths of a second (0.01 seconds). The minimum and default values are 1, corresponding to a delay of 0.01 seconds; the maximum value is 50, corresponding to a delay of 0.5 seconds. HPE recommends an initial value of 50. However, the optimum setting depends on your system, and you can change the value as necessary to optimize the performance.
2. Save the changes to the PDESC using the procedure in the *Configuration Procedures Guide*.

#### 5.3 Diameter service activation limitation

---

A host name cannot be resolved to an IP address on the Telco CLIM. Therefore, the Diameter service fails upon activation when a host name, rather than an IP address, is used as part of the Diameter host's URI.

```
Example: aaa://fred.nodeb.nbn.usa.hp.com:3868;TRANSPORT=TCP
```

The Diameter service can only start successfully when the Diameter host's URI contains an explicit IP address.

```
Example: aaa://16.125.241.20:3868;TRANSPORT=TCP
```

## 5.4 File code 100 object files are not supported

---

The code 100 (non-native, CISC format) executable/user-application, which uses the INS libraries, is not supported from INS 06.00.00 release onwards.

## 5.5 Limitation on number of processes to be run

---

For a specific task ID and server-class combination, a maximum of 31 processes can be run per processor.

## Chapter 6

### Known issues

---

#### 6.1 Front-back node configuration migration is not working during node installation

---

<b>Case ID and severity</b>	<b>10-190515-1057 Minor (E)</b>
Reported in release	INS 09.00.00
Description	Front-back node configuration migration is not working during node installation procedure.
Workaround	Use MIGCFG, the migration tool present in the aaansa01 subvolume, for frontnode-backnode migration.

#### 6.2 Accessing CCMI using HTTP URL, when CCMI is configured to run on HTTPS causes log file to be filled up

---

<b>Case ID and severity</b>	<b>10-180822-1097 Minor (E)</b>
Reported in release	INS 08.02.02
Description	Accessing CCMI using HTTP URL, when CCMI is configured to run on HTTPS, causes log file on guardian side to be filled up with error messages. This log file is updated by UICM process.
Workaround	None

#### 6.3 Remote operations on 64-BIT protect contexts are not functioning properly

---

<b>Case ID and severity</b>	<b>10-150220-2504 Major (I)</b>
Reported in release	INS 07.00.10
Description	Remote operations on 64-bit protect contexts may not function properly.
Workaround	Restart the node.

#### 6.4 Diameter command code routing feature does not work as expected

---

<b>Case ID and severity</b>	<b>10-140806-6874 Minor (I)</b>
Reported in release	INS 07.00.01

Description	Requests are distributed in a round-robin manner across the configured Task-ID and server class even though Command Code Routing is enabled.
Workaround	None

## 6.5 Alarms in CCMI getting truncated when it is more than 3 lines

---

<b>Case ID and severity</b>	<b>10-130924-9382 No Impact (I)</b>
Reported in release	INS 06.02.11
Description	The INS CCMI can only display a maximum of three lines of ERAD text. The text gets truncated if it exceeds three lines.
Workaround	None

## 6.6 Fault management screen of UI pathway does not show the full EMS text from \ZLOG

---

<b>Case ID and severity</b>	<b>10-130918-5095 No Impact (I)</b>
Reported in release	INS 06.02.10
Description	The Fault Management screen can only display a maximum of three lines of ERAD text. The text gets truncated if it exceeds three lines.
Workaround	None

# Chapter 7

## Installation instructions

---

### 7.1 Important notes for Installation

---

#### 7.1.1 Process Input Parameter RTR-REPLY-SIZE

Based on the need of the application, the parameter RTR-REPLY-SIZE should be tuned.

If the application reply message size is more than the Router Reply Size, then the message is not routed out but discarded with the MTS error (ERAD category 02, ERAD number 5259).

```
DDDDDDDDDD 2012-09-11 11:36:14 32117 HOST0002 SOFT 5259 32118 $HS2D0
MTS Invalid message transfer count encountered.
MTS REPLY operation, Xfer count: (9692)

DDDDDDDDDD 2012-09-11 11:36:14 32118 HOST0002 HSS_ 0193 32119 $HS2D0
** Routine: ULR st_reply() sendToSession() for
reply failed rc: 8
HSS_ 0193 OFF
```

For more information on the parameter, see Section 4.3.13.2, “Router Reply Size Parameter” of the Configuration Planning Guide.

#### 7.1.2 Setting the Value of Max Path Retrans

For Diameter services, which are migrated from earlier releases (with default INS SCTP parameters), the value of ‘Max. Path Retrans’ SCTP parameter, configured in the fourth page of Diameter Service screen, should be changed to 5 to avoid ERADs such as the following:

```
YYYYYYYYYYY 2012-09-13 03:53:54 22704 HOST0001 SOFT 9820 22705 $S7MOZ
CLIM To Host Port: $ZTC5:22848
Diameter Transport setsockopt(SCTP_ASSOCINFO) failed: (22)
```

For newly added services, the default value of ‘Max. Path Retrans’ is 5.

#### 7.1.3 Process Input Parameter SEGMENT-SIZE

The interpretation of the process input parameter SEGMENT-SIZE by the context subsystem has changed. The value of the parameter is now specified in megabytes instead of bytes.

Refer to the Configuration Procedures Guide and the Configuration Planning Guide to ensure that the parameter values are appropriate.

## 7.1.4 CLIM Parameter Settings for CLIM OS Version ABA or greater

If the CLIM OS version used is T0853H01\_16AUG2010\_14JUL2010\_ABA or greater, then the following SCTP parameter needs to be set before using the CLIM.

### 7.1.4.1 New Kernel Parameter for SCTP: “net.sctp.addip\_noauth\_enable”

Default Value: 0

Purpose: Dynamic Address Reconfiguration (ADD-IP) requires the use of authentication to protect the operations of adding or removing new addresses. This requirement is mandated so that unauthorized hosts would not be able to hijack associations. However, older implementations may not have implemented this requirement while allowing the ADD-IP extension. For reasons of interoperability, we provide this variable to control the enforcement of the authentication requirement.

1 - Allow ADD-IP extension to be used without authentication. This should only be set in a closed environment for interoperability with older implementations.

0 - Enforce the authentication requirement

Impact: If left to default, that is, 0, then sctp-init will be aborted if peer supports ASCONF capability.

For Diameter services, we do change a few of the connection parameters (for example, setting the primary peer), which is communicated using the ASCONF message. For communicating the ASCONF message, both sides “net.sctp.addip\_enable” should be set to one. If the “net.sctp.addip\_enable” is set to one and “net.sctp.addip\_noauth\_enable” is set to zero, then SCTP INIT would be aborted.

Recommendation: To set the “net.sctp.addip\_noauth\_enable” parameter to “1” for the INS Diameter services.

Configuration Steps:

1. Login as SUPER.SUPER.
2. On the TAACL prompt, run:

```
CLIMCMD <CLIM-NAME> CLIMCONFIG sysctl -update net.sctp.addip_noauth_enable 1
```

### 7.1.4.2 New Kernel Parameter for SCTP: “net.sctp.addr\_scope\_policy”

Default Value: 1

Purpose: This is to control the scoping of IP address used (for IPv4 defined in <http://tools.ietf.org/id/draft-stewart-tsvwg-sctp-ipv4-00.txt>).

0 - Disable IPv4 address scoping

1 - Enable IPv4 address scoping

2 - Follow draft but allow IPv4 private addresses

3 - Follow draft but allow IPv4 link local addresses



**Impact:** If left with default settings, then the SCTP association for the public IP address to private IP address (Private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) can't be done.

**Recommendation:** Based on the security recommendation at customer site where policy setting can be decided with appropriate IP address configuration.

**Configuration Steps:**

1. Login as SUPER.SUPER
2. On the TAcl prompt, run:

```
CLIMCMD <CLIM-NAME> CLIMCONFIG sysctl -update net.sctp.addr_scope_policy <Security Recommendation Value At Customer Site>
```

Where <Security Recommendation Value at Customer Site> could be one the following:

- 0 - Disable IPv4 address scoping
- 1 - Enable IPv4 address scoping
- 2 - Follow draft but allow IPv4 private addresses
- 3 - Follow draft but allow IPv4 link local addresses

### 7.1.4.3 Kernel Parameter for SCTP: "net.sctp.auth\_enable"

**Default Value:** 1

**Purpose:** Parameter to enable authentication feature in SCTP. This parameter needs to be set to 1 for DTLS over SCTP connections.

- 0 - Disable authentication feature of SCTP
- 1 - Enable authentication feature of SCTP

**Impact:** If left to default, that is 0 then the DTLS over SCTP connection abort.

**Recommendation:** By default, this parameter is set to 1 when the INS CLIM Packages are installed. To set the "net.sctp.auth\_enable" parameter to "1" for INS Services.

**Configuration steps:**

1. Login as SUPER.SUPER
2. On the TAcl Prompt, run:

```
CLIMCMD <CLIM-NAME> CLIMCONFIG sysctl -update net.sctp.auth_enable 1
```

## 7.2 Installation considerations

### 7.2.1 Installing CLIM software

If the CLIM software is delivered as a component of this release, follow the instructions in the *HPE INS Installation Guide*, Appendix F, “CLIM Configuration”, subsection “INS CLIM Software Installation.”

To ensure correct installation of the CLIM package provided with the IPM, see the protocol package versions provided in the [CLIM OS](#) section.

To list the CLIM protocol package version, use the command provided in the [Identifying existing SIP package](#) section.



**NOTE:** Multiple versions of the SIGTRAN (M3UA/SCTP) software may be used on a single CLIM. From INS 07.00.00 onwards, multiple versions of Diameter software may also be used on a single CLIM. Only one version of the SIP software can be used on each CLIM. If multiple versions of the SIP software are installed on a CLIM, the CLIM will use the latest version. Later versions of the SIP software may not be compatible with the earlier versions of the INS software. Make sure that the SIP software in use is compatible with the INS software that is using the CLIM for SIP sessions.

#### 7.2.1.1 Identifying existing SIP package

The following command lists the existing packages installed on the CLIM for SIP package.

```
CLIMCMD <clim-name> dpkg -l ~| grep -i sip
```

Example output:

```
*SS*\TAXILA.$SK8110.AAANSA01 6> CLIMCMD o1002571 dpkg -l ~| grep -i sip
ii hpesip 1.0.0-737
amd64 HPE SIP Stack libraries
ii ins-clim-sip-8.1.10 8.1.10-6218
amd64 INS CLIM SIP protocol support
```

If the command lists a SIP package, remove the package completely by using the procedure in section [Remove Existing INS SIP CLIM Packages](#).

#### 7.2.1.2 Removing existing INS SIP CLIM packages



**NOTE:** You need to remove an existing INS SIP CLIM package only if the version of the existing package is higher than the version of the package provided with this INS release.

To completely remove the previously installed packages along with the configuration files and dependent libraries on the CLIM, use the following commands.

1. Logon as `SUPER.SUPER`.
2. At the `NSK TACL` prompt, type the commafeaturends as shown below and make sure that the `<release _version>` specified in the commands is the INS release version identified in the previous section.

```
Example: CLIMCMD <clim-name> clinsupdate remove ins-clim-core-5.3.12.
```

```
CLIMCMD <clim-name> clinsupdate remove ins-clim-core-<ins-release-version>
CLIMCMD <clim-name> clinsupdate remove ins-clim-sip-<ins-release-version>
CLIMCMD <clim-name> clinsupdate remove hpesip
CLIMCMD <clim-name> clinsupdate remove hpebus
CLIMCMD <clim-name> clinsupdate remove hpegmf
CLIMCMD <clim-name> clinsupdate remove hpctbx
CLIMCMD <clim-name> clinsupdate remove ins-clim-nodeppm-<ins-release-version>
CLIMCMD <clim-name> clinsupdate remove ins-clim-vproc
```

3. If the package is removed successfully, you see the following output for each of the above operations.

```
comForte SSH client version T9999H06_07Jan2010_comForte_SSH_0087
CLIM_INS_UPDATE_SUCCESS
Termination Info: 0
```

4. If SIP packages were installed from NonStop Console, make sure that the packages are also deleted from the console.

### 7.2.1.3 Installing a new SIP package

Once you have removed the packages, install the SIP package to the CLIM given in the release by using the following commands:

```
VOLUME $<INSNODE>.AAANSA01
INSTCLIM <clim-name> ins-clim-sip-9.1.30
```



**NOTE:** In case of problems in INSTCLIM, please review `/etc/apt/sources.list` file on CLIM to make sure it is pointing to correct console IP address.

## 7.3 Database information

Modifications to HPE INS NSDB:	Yes
Modifications to HPE INS ERAD database:	No
Modifications to HPE INS SS7 database:	No
Modifications to HPE INS SIP database:	No
Modifications to HPE INS Diameter database:	Yes
Modifications to HPE INS EMS templates:	No
Modifications to HPE INS statistics:	Yes
Modifications to HPE INS libraries:	Yes
Modifications to HPE INS User Interface:	No

## 7.4 Node installation instructions

---



**NOTE:** Third-party applications often require the use of the INS libraries to compile and execute properly. Third-party applications can run either under the INS node or externally and then attach to the node. Applications not controlled by the INS node might hold the INS library objects open, even though the node has been shut down as instructed. Prior to performing any migration installation, ensure that all libraries in the CSSLIB sub-volume are not open. If any of the libraries are open, shut down or ensure shutdown of the application holding the library or libraries open. This will release the library and allow proper completion of the installation.

---

1. Follow the instructions in the *HPE INS Installation Guide*, Section 4, “Full Maintenance and IPM Installations”, to install the node software.
2. Follow the instructions in the *HPE INS Installation Guide*, Appendix F, “CLIM Configuration”, to install the CLIM software.



**NOTE:** The “package ID” referred to in the *HPE INS Installation Guide*, Appendix F, see one of the following:

- ins-clim-m3ua-9.1.30
  - ins-clim-sip-9.1.30
  - ins-clim-diameter-9.1.30
  - ins-clim-mon
- 

3. INS Telco CLIM Installation Software  
Version: T8718H06^0991T08^IINS\_R09\_01\_30

## 7.5 Performing a backout

---

If a backout is necessary, perform the following steps:

1. Shut down the INS node, the user interface, ERAD subsystems, and all associated node processes.
2. Follow the *HPE INS Installation Guide* instructions for backing out of a node installation.
3. Restart the node and all associated processes.