

```

*****
3625 Mon Jan 13 01:00:22 2020
new/usr/src/man/man7d/n2rng.7d
12186 The n2rng man page incorrectly refers to n2cp
*****
1 \" te
2.\" Copyright (c) 2009 Sun Microsystems, Inc. All Rights Reserved.
3.\" Copyright (c) 2020 Peter Tribble.
4.\" The contents of this file are subject to the terms of the Common Development
5.\" See the License for the specific language governing permissions and limitat
6.\" the fields enclosed by brackets "[" replaced with your own identifying info
7.TH N2RNG 7D "Jan 12, 2020"
6.TH N2RNG 7D "Apr 15, 2009"
8.SH NAME
9 n2rng \- Ultra-SPARC T2 random number generator device driver
10.SH DESCRIPTION
11.LP
12 The \fBn2rng\fR device driver is a multi-threaded, loadable hardware driver
13 supporting hardware assisted random numbers.
14 This support is built into the Ultra-SPARC T2 and later processors.
15 supporting hardware assisted random numbers. This support is built into the
16 Ultra-SPARC T2 CMT processor.
17.LP
18 The \fBn2rng\fR driver requires the presence of the Solaris Cryptographic
19 Framework to enable applications and kernel clients to access the provided
20 services.
21.SH CONFIGURATION
22.LP
23 You configure the \fBn2rng\fR driver by defining properties in
24 \fB/platform/sun4v/kernel/drv/n2rng.conf\fR which override the default settings.
25 \fB/platform/sun4v/kernel/drv/n2cp.conf\fR which override the default settings.
26 The following property is supported:
27.LP
28.ne 2
29.na
30 \fBnostats\fR
31.ad
32.RS 28n
33 Disables the generation of statistics.
34 The nostats property may be used to help prevent traffic analysis, however,
35 this may inhibit support personnel.
36 Disables the generation of statistics. The nostats property may be used to help
37 prevent traffic analysis, however, this may inhibit support personnel.
38.RE
39.SH CRYPTO STATISTICS
40 Solaris crypto drivers must implement statistics variables.
41 Statistics reported by \fBn2rng\fR may be read using the \fBkstat\fR(LM)
42 utility.
43 The \fBn2rng\fR driver maintains the following statistics:
44.LP
45 Solaris crypto drivers must implement statistics variables. Statistics are
46 reported by \fBn2rng\fR using the \fBkstat\fR(7D) and \fBkstat\fR(9S)
47 mechanisms. The \fBn2rng\fR driver maintains the following statistics:
48.LP
49.ne 2
50.na
51 \fBstatus\fR
52.ad
53.RS 28n
54 Status (online, offline, fail) of RNG device.
55.RE

```

```

48 .sp
49 .ne 2
50 .na
51 \fBBrngjobs\fR
52 .ad
53 .RS 28n
54 Number of requests for random data.
55 .RE

57 .sp
58 .ne 2
59 .na
60 \fBBrngbytes\fR
61 .ad
62 .RS 28n
63 Number of bytes read from the RNG device.
64 .RE

66 .SH KERNEL STATISTICS
70 .sp
71 .LP
72 The \fBn2rng\fR driver tallies a set of kernel driver statistics when in the
73 Control domain.
74 Statistics reported by \fBn2rng\fR may be read using the \fBkstat\fR(LM)
75 utility.
76 Control domain. Statistics are reported by \fBn2rng\fR using the
77 \fBkstat\fR(7D) and \fBkstat\fR(9S) mechanisms. All statistics are maintained
78 as unsigned, and all are 64 bits.
79.LP
80 .sp
81 .ne 2
82 .na
83 \fBBrng(n)-cell0-bias\fR
84 .ad
85 .RS 28n
86 Bias setting for noise cell 0 of RNG \fIn\fR.
87 .RE

89 .sp
90 .ne 2
91 .na
92 \fBBrng(n)-cell1-bias\fR
93 .ad
94 .RS 28n
95 Bias setting for noise cell 1 of RNG \fIn\fR.
96 .RE

98 .sp
99 .ne 2
100 .na
101 \fBBrng(n)-cell1-entropy\fR
102 .ad
103 .RS 28n
104 Entropy value for noise cell 1 of RNG \fIn\fR.
105 Entropy value for noise cell 1 of RNG n.
106 .RE

```

```

107 .sp
108 .ne 2
109 .na
110 \fBBrng(n)-cell2-bias\fR
111 .ad
112 .RS 28n
113 Bias setting for noise cell 2 of RNG \fIn\fR.
114 .RE

```

```

116 .sp
117 .ne 2
118 .na
119 \fBBrng(n)-cell2-entropy\fR
124 \fBBrng(n)-cell3-entropy\fR
120 .ad
121 .RS 28n
122 Entropy value for noise cell 2 of RNG \fIn\fR.
123 .RE

```

```

125 .sp
126 .ne 2
127 .na
128 \fBBrng(n)-state\fR
129 .ad
130 .RS 28n
131 State of rng number n (online, offline, error, health check).
132 .RE

```

134 .SH FILES

```

140 .sp
135 .ne 2
136 .na
137 \fB/platform/sun4v/kernel/drv/sparcv9/n2rng\fR
143 \fB/platform/sun4v/kernel/drv/sparcv9/n2cp\fR
138 .ad
139 .sp .6
140 .RS 4n
141 Device driver (SPARC)
147 64-bit ELF kernel driver.
142 .RE

```

```

144 .sp
145 .ne 2
146 .na
147 \fB/platform/sun4v/kernel/drv/n2rng.conf\fR
153 \fB/platform/sun4v/kernel/drv/n2rng.conf\fR
148 .ad
149 .sp .6
150 .RS 4n
151 Driver configuration file
157 Configuration file.
152 .RE

```

154 .SH ATTRIBUTES

```

161 .sp
162 .LP
155 See \fBAttributes\fR(5) for descriptions of the following attributes:
156 .sp

```

```

158 .sp
159 .TS
160 box;
161 c | c
162 l | l .
163 ATTRIBUTE TYPE ATTRIBUTE VALUE
164 _

```

```

165 Architecture SPARC
166 _
167 Interface stability Committed
168 .TE

```

```

170 .SH SEE ALSO
171 \fBcryptoadm\fR(1M), \fBkstat\fR(1M), \fBAttributes\fR(5)
179 .sp
180 .LP
181 \fBcryptoadm\fR(1M), \fBkstat\fR(1M), \fBprinters.conf\fR(4),
182 \fBAttributes\fR(5)
183 .sp
184 .LP
185 \fISolaris Cryptographic Framework - Solaris Software Developer Collection\fR
186 .sp
187 .LP
188 \fISolaris Security for Developer's Guide - Solaris Software Developer
189 Collection\fR

```