INFO925 "%1$s: None of the host identities currently supported by the local\n
system are associated with the current public key value used by the local\n
system. This can cause authentication failures for an application on the local\n
system if it attempts to contact a service on the local system through a\n
network communication channel. The trusted host list file used in this test is\n
listed below:\n
\t Trusted host list file: %2$s\n
The public key value was obtained from the following file:\n
\t   Public key file: %3$s\n
If the %4$s and %5$s options were specified, ensure that the correct trusted\n
host list file path name and public key file path name were used. If the\n
correct file path names were used, the system administrator must perform\n
further investigation to determine whether it is the public key file or the\n
trusted host list file is in error.\n
\t One means for making this determination is to check the public key\n
value listed for the local system on another system that regards the local\n
system as a trusted host, using the ctsthl command on the other system.\n
This value can be compared to the value obtained from the ctskeygen -d command\n
on the local system. If these values agree, then it is likely that the local\n
trusted host list file is in error. The incorrect entry can be modified to\n
use the correct public key value using the ctsthl command on the local system.\n
The list of identities associated with incorrect public key values can be\n
obtained by issuing the %1$s command with the most detailed output option\n
enabled.\n"
$ arguments:command name; path name of trusted host list file; command line
$ option to specify the trusted host list file path name
$ explanation: At least one of the host identities supported by the local
$ system was located in the trusted host list file, but those
$ entries are not associated with the correct public key value.
$ actions: Consult the test of the message.
t %2$s\n
EMSG930 "Failure: The command was unable to obtain the local\n
host identity information necessary for the Host Based Authentication (HBA)\n
security mechanism to correctly identify this system to a remote system.\n
This failure may be the result of poor network performance between the local\n
system and the network domain name server, by poor performance on the domain\n
name server, or by network host name resolution configuration problems.\n
Perform the proper problem determination procedures to identify and repair\n
host name resolution and domain name service problems.\n
Repeat this command\n
at a later time.\n
$ arguments:Command name
$ explanation: The command was unable to fully resolve the local system's
$ primary host name through domain name services.
$ actions: Consult the test of the message for the appropriate actions to
$ take in response to this message.
$
INFO924 "%1$s: A host naming discrepency has been detected that can cause\n
failures in Host Based Authentication mutual authentication processing.\n
The fully resolved host name for the local system is listed below.\n
\t %2$s\n
This name was obtained by resolving the value returned by the gethostname()\n
C library routine. However, this name was not obtained when the host names\n
for all active network addresses were obtained. Because a matching value\n
was not found, mutual authentication can fail in certain conditions. The\n
host name and address resolution capability of the local system should be\n
modified so that the same fully resolved host name value is obtained for\n
both the local system name and at least one of the currently active network\n

interfaces.\n"
EMSG929 "2650-929 %1$s Failure: The private key file has a configuration\n
problem. The private key file used by this command resides in the following\n
location:\n
\t Private key file path name: %2$s\n
For further detail on the nature of the configuration problem, issue the\n
%1$s command with the most detailed output option enabled. The\n
appropriate corrective action will depend on the nature of the configuration\n
problem.\n
\t * For user access failures, ensure that the correct system\n
\t   user is issuing this command.\n
\t * For other conditions, ensure that the correct private\n
\t   key file path name is specified in the %3$s option or the\n
\t   configuration file. If the file path name is correct,\n
\t   the system administrator should consider generating a\n
\t   new pair of private and public keys using the ctskeygen\n
\t   command and replacing the entries for the local system in\n
\t   the trusted host list file using the ctsthl command.\n
\t   System administrators should remember that when these\n
\t   keys are regenerated for a node, all systems that consider\n
\t   the local system a trusted host must be informed of the\n
\t   public key value change and update their trusted host lists\n
\t   accordingly.\n
\t * If the command cannot determine the private key file status,\n
\t   the file system may require further manual examination.\n"
EMSG928 "2650-928 %1$s Failure: The public key file has a configuration\n
problem. The public key file used by this command resides in the following\n
location:\n
\t Public key file path name: %2$s\n
For further detail on the nature of the configuration problem, issue the\n
%1$s command with the most detailed output option enabled. The\n
appropriate corrective action will depend on the nature of the configuration\n
problem.\n