BoKS Manager 6.7 Release Notes

This document contains information about the BoKS Manager 6.7 product release from Fox Technologies. It includes the following sections:

- Revision History
- Supported Platforms
- What's New
  - Revision A3 Package
  - SSH Kerberos Password Authentication
  - Support for MIT Kerberos
  - SSH User Public Key Management
  - Automatic Creation of Home Directory
  - boks_sshd Uses PAM to Set up User Environment
  - New suexec safepath Modifier
  - System Performance Monitoring Activated
  - New kerberos_allow_ticket Modifier, preauth Modifier Deprecated
  - AD Bridge Support For Windows Domain Users in BoKS
  - Admin Server Integrated With BoKS Master
- What's Changed
  - OpenSSH Upgrade
  - Changes to BoKS ENV Variables, Monitoring Functions
  - SSOUSERS no Longer Created by Default
- Fixed Issues
  - Fixed Issues on All Platforms
  - Fixed Issues on IBM AIX
  - Fixed Issues on Red Hat
  - Fixed Issues on Red Hat 5
  - Fixed Issues on Red Hat 6
  - Fixed Issues on Oracle Solaris
  - Fixed Issues on Oracle Solaris 11
  - Fixed Issues on SuSE Linux
  - Fixed Issues on VMWare 4.0-4.1
- Known Issues

- Known Issues on All Platforms
- Known Issues on IBM AIX
- Known Issues on IBM AIX 6.1
- Known Issues on HP-UX
- Known Issues on HP-UX 11iv2 & 11iv3
- Known Issues on Red Hat
- Known Issues on Red Hat 7
- Known Issues on Red Hat 6 and 7
- Known Issues on Red Hat 6
- Known Issues on Oracle Solaris 11
- Known Issues on Debian 7 / Ubuntu 12
- Known Issues on Ubuntu 12

- Getting Support And Service

Revision History

Revision: 13

Date of this revision: 12/11/2018

Revision history:

Rev No	Date	Comments
1	09/20/2013	First version.
2	10/18/2013	Added platform support for CentOS 6.
3	03/17/2014	Added several fixed issues, platform support for Oracle Enterprise Linux.
4	04/16/2014	Added information on hotfix for SELinux on RHEL6.
5	07/02/2014	Removed desupported platforms.
6	09/10/2014	Added information about revision A2, and Server Agent support for Cumulus Linux.
7	09/17/2014	Added information about revision A3.
8	10/20/2014	Added platform support for RHEL 7, Oracle Enterprise Linux 7 and CentOS 7.
9	11/17/2014	Added platform support for Debian 7, Ubuntu 12.
10	05/06/2015	Added known issue #8205, EoL information.
11	11/19/15	Added platform support for RHEL 6 on zSeries (Server Agent only).

Rev No	Date	Comments
12	03/08/17	Added information about BoKS SELinux policy RPM and hotfixes HFBM-0164 / HFBM-0167.
13	12/11/2018	Added information about Oracle Solaris 11 support.

Go to top

Supported Platforms

BoKS Manager 6.7 is supported on the following platforms:

Vendor	Platform	Comments
HP	HP-UX 11.11 (v1), 11.23 (v2), 11.31 (v3) for PA-RISC	Server Agent only.
	HP-UX 11.23, 11.31 for Intel Itanium HP-UX nPartitions, Virtual Partitions and Integrity VM	Server Agent only. List of HP-UX virtualization modes tested for the FoxT Server Agent package for HP-UX 11 Itanium
IBM	IBM AIX 7.1	
	IBM AIX 6.1	AIX 6.1 requires Service Pack 2 (6100-00 Service Pack 2) or higher
Microsoft	Microsoft Windows Server 2003, R2 or later (32 & 64 bit)	Server Agent only. BoKS Server Agent for Windows 6.7.
	Microsoft Windows Server 2008 R2 or later (64 bit)	Server Agent only. BoKS Server Agent for Windows 6.7.
	Microsoft Windows Server 2012	Server Agent only. BoKS Server Agent for Windows 6.7.
Oracle	Oracle Solaris 11 on SPARC & x64	Oracle Solaris up to and including v 11.3 is supported. Oracle Solaris 11.4 is not supported.
	Oracle Solaris 10 on SPARC, x86 & x64	
	Oracle Enterprise Linux 7‡	Server Agent only. Support for this platform is included in the package for Red Hat EL 7.0
	Oracle Enterprise Linux 6	Server Agent only. Support for this platform is included in the package for Red Hat EL 6.0
	Oracle Enterprise Linux 5	Server Agent only. Support for this platform is included in the package for Red Hat EL 5.0

Vendor	Platform	Comments
Red Hat	Red Hat Enterprise Linux 7 on x64‡	Server Agent only.
	Red Hat Enterprise Linux 6 on x64	
	Red Hat Enterprise Linux 6 on x86	Server Agent only.
	Red Hat Enterprise Linux 6 on zSeries	Server Agent only.
	Red Hat Enterprise Linux 5 on x64	
	Red Hat Enterprise Linux 5 on x86	Server Agent only.
SUSE from Novell	SUSE Linux Enterprise Server 11 on x64	
	SUSE Linux Enterprise Server 11 on x86 & zSeries	Server Agent only.
CentOS	CentOS 7 on x64‡	Server Agent only. CentOS 7 support included in the BoKS Manager package for Red Hat Enterprise Linux 7 on x64
	CentOS 6 on x64	Server Agent only. CentOS 6 support included in the BoKS Manager package for Red Hat Enterprise Linux 6 on x64
Cumulus	Cumulus Linux 2.1 (Debian-based)	Server Agent only. See the *BoKS Manager 6.7 Debian Release Notes* for specifics. This package is available at the Cumulus online repository - please contact your Fox Technologies representative for details.
Debian	Debian 7 on x86	Server Agent only.
Ubuntu	Ubuntu 12 on x64	Server Agent only.

‡ Note that for the Red Hat 7 / Debian 7 / Ubuntu 12 package, you do not need to install the BoKS hotfixes HFBM-0039, HFBM-0043 and HFBM-0047. These hotfixes include updates to third-party components such as OpenSSL, and the updated versions of the components are already included in the Red Hat 7 package.

Go to top

End-of-life Information

This release has the following end-of-life schedule:

Support Phase	End Date
Production phase 1 - Feature enhancements, hotfixes and security fixes.	May 31, 2019
Production phase 2 - Critical hotfixes and security fixes.	May 31, 2021
Production phase 3 - Security fixes.	May 31, 2022

What's New

New features in this release.

A note on administration interfaces: New functionality is managed by the CLI or FoxT Control Center. It is not supported in the BoKS Administration GUI shipped together with BoKS Manager. Note that the BoKS Administration GUI is not activated by default when you install BoKS Manager 6.7, and must be activated by setting the BoKS ENV variable HTTPSRV to "on" and restarting BoKS on the BoKS Master.

Note: The BoKS Administration GUI is no longer supported and is deprecated functionality. It may not be included in future releases of BoKS Manager.

Revision A3 Package

A new BoKS Manager 6.7 package, revision A3, is available for download from the Fox Technologies customer support website. This revision includes a new version of the `install` program produced to fix an issue in the previous package. For details on the install issue this revision fixes, see the description under TFS140721-015009, TFS140827-015078.

Note that revision A3 is a replacement for revision A2, which includes a solution for the known issue #7530 found in revision A2. For details of the issue, see #7530.

Note: The revision A3 package does NOT need to be installed to replace existing installations of BoKS Manager 6.7 / BoKS Server Agent for Unix/Linux 6.7. The only change in this package is the new version of the `install` program. Fox Technologies recommends that this package is used for new installations of BoKS Manager 6.7 / BoKS Server Agent for Unix/Linux 6.7.

SSH Kerberos Password Authentication

User accessing Unix servers via SSH can be allowed to authenticate using their Kerberos password in addition to authenticating via a Kerberos ticket as has been supported in previous versions.

Support for MIT Kerberos

BoKS Manager 6.7 includes support for MIT Kerberos, and has been tested and verified to function with MIT Kerberos for user authentication.

SSH User Public Key Management

BoKS Manager 6.7 includes functions for the centralized management of user SSH Public Keys including key provisioning and self-service registration by users, all managed through BoKS access controls.

Automatic Creation of Home Directory

Automatic creation of home directory at SSH login is now also available in privileged separation mode if:

- The user's home directory does not exist.
- CREATE_HOMEDIR_PATH is set in the local ENV file.
- Offline mode is not enabled.
- The login does not include a chroot operation.

boks_sshd Uses PAM to Set up User Environment

On all PAM platforms except for HP-UX, boks_sshd uses PAM to access the user environment set up on the host to control shell limits etc.

New suexec safepath Modifier

SUEXEC Access Routes can now be specified with the modifier "safepath" which applies stricter checking of permissions on the executed program and all the directories in the path.

System Performance Monitoring Activated

The system performance monitoring features in BoKS Manager are activated when you install BoKS Manager 6.7 and cannot be deactivated. For more information on the features, see Appendix C "System Monitoring Tools" in the BoKS Manager Administration Guide.

New kerberos_allow_ticket Modifier, preauth Modifier Deprecated

A new modifier has been added for SU and SUEXEC Access Routes that use Kerberos authentication. kerberos_allow_ticket can be set to allow users to perform SU or SUEXEC using a ticket obtained at an earlier authentication to Active Directory, rather than having to authenticate again by supplying their Kerberos password. The preauth modifier which was included in BoKS Manager 6.6.2 is now deprecated and should not be used.

AD Bridge Support For Windows Domain Users in BoKS

This release adds the capability to create Windows Domain account types in BoKS by synchronizing account information from Active Directory using the AD Bridge function. For more information see the BoKS Manager Administration Guide.

Admin Server Integrated With BoKS Master

The admin server used for managing BoKS via FoxT Control Center, which was previously installed as a separate extension package on the Master, is now included in the BoKS Manager installation package and installed together with BoKS Manager.

Go to top

What's Changed

Changed features in this release.

OpenSSH Upgrade

OpenSSH has been upgraded from version 5.6p1 (in BoKS 6.6) to version 6.1p1.

sshd Setup During Installation

An sshd user and an sshd group are now always created during the BoKS installation.

Changes to BoKS ENV Variables, Monitoring Functions

A number of BoKS ENV variables have an updated default setting, and some ENV variables have become obsolete in version 6.7. These obsolete variables relate to file location for system monitoring files, which have now been consolidated into the one parameter MONITORING_DIR which is set by default to $BOKS_var/monitoring. In addition, system monitoring of BoKS processes is now activated by default and cannot be deactivated. For more information, see the BoKS man page ENV, and the BoKS Manager Administration Guide.

SSOUSERS no Longer Created by Default

The User Class SSOUSERS is no longer created by default when installing a BoKS Master. If this User Class is required is must be created manually after installation. If the installation is an upgrade, the SSOUSERS User Class might be created when restoring the database backup taken before the upgrade.

Go to top

Fixed Issues

Issues that have been fixed in this release.

Fixed Issues on All Platforms

TFS140721-015009, TFS140827-015078

install PROGRAM FAILS IF BCASTADDR FILE HAS SECONDARY_ADDRESS_LIST DEFINED

The `install` program fails if it is given a `bcastaddr` file as an argument and the `bcastaddr` file includes the parameter `SECONDARY_ADDRESS_LIST`.

#6535, TFS120606-013543

BoKS TREATS UID/GID AS SIGNED ON LINUX

BoKS treats user uid/gids as signed values on all operating systems except IBM AIX, where it is treated as an unsigned value, but in fact uid/gid is also an unsigned value on Red Hat and SuSE. This causes the uid/gui on Red Hat and SuSE to be written as a negative value if greater than 2147483647.

#6516, TFS130403-014165

HOST GROUP CHANGE VIA ldapsync DENIED

The `m odbks` program includes a restriction to prevent the Host Group being changed in BoKS for users imported from LDAP. However this restriction means that import of users whose Host Group has been changed on the LDAP side does not work. In addition, calling `m odbks` with the argument `-g` may cause the program to dump core.

#6406, TFS120911-013787

boks_dbupdate_reader CAUSES NULL-POINTER EXCEPTION

When FoxT Reporting Manager was in use, boks_dbupdate_reader sent empty data to be processed by the java component, causing a null- pointer exception error.

#6405, TFS120808-013700

LONG BRIDGE ERROR RECOVERY TIME WHEN MANY MESSAGES QUEUED

If there were many messages in the batch queue to the Master on a Replica and the Master sent a communication error to the Replica in a message, the bridge took a long time to recover from the error.

#6382, TFS131018-014492

lsbks DOES NOT DISPLAY PRIMARY USER CLASS ACCESS ROUTES

If you assign a primary User Class using the command modbks -P to a user who did not previously have one, Access Routes inherited by the user from this User Class are not displayed when you run the lsbks command.

#6253, TFS130206-014049

aced API TRUNCATES USERNAME

The API used for communication with aced from other programs truncated the input username to 31 characters, causing errors.

#6223, TFS130213-014060

boksinfo TO COLLECT STATUS FOR SELinux

The boksinfo utility did not include status information for SELinux. Now boksinfo reports on configuration and status for SELinux in the files selinux_conf.txt and selinux_status.txt.

#6193

SHOULD NOT BE ABLE TO MAP MULTIPLE UPNS TO ONE BoKS USER

It should not be possible to map multiple different Kerberos UPNs to one BoKS user account.

#6164, TFS090410-074318

FILMON STATUS FILE OCCASIONALLY TRUNCATED

The file $BOKS_var/filmon/boks.db, which keeps track of the status of monitored files for file monitoring, occasionally became truncated.

#6163, TFS090116-140439

LOG ROLLOVER SHOULD NOT BE ALLOWED ON A REPLICA

It was possible to start a new log on the Master using the logadm program from a Replica, and this should not be allowed.

#6162, TFS101221-012249

mkvc DUMPS CORE ON DOUBLE FREE

When creating a host virtual card using the vcgen utility, vcgen calls mkvc. If the nodekey had not been set in BoKS, mkvc performed a double free operation and dumped core.

#6160, TFS090721-104643

BRIDGE PID FILES NOT USED AS LOCK

BoKS bridge daemons did not use the same process locking behavor as other daemons, leading to anomalies.

#6159, TFS091207-151055

servc DOES NOT OBEY PID FROM LOCK FILE

The servc* process lock files did not contain the correct pids for the processes.

#6158, TFS091118-144656

NFS SUPPORT MISSING IN FILMON

File monitoring failed to open a read-only file, because it did not include support for NFS mounted files.

#6157, TFS101011-011966

MISMATCHING NODEKEY ERROR NOT LOGGED

No warning was printed to boks_errlog from boks_bridge when a nodekey mismatch occured (i.e. there was a difference between the nodekey stored in $BOKS_etc/nodekey and that in the BoKS database).

#6154, TFS051221-100754

COMMUNICATION ERROR FOR sshd MAY CAUSE ACCOUNT LOCKOUT

If communication with BoKS failed and access control information could not be retrieved at a user Public Key authentication, and the client was started from a batch script, sshd tried to log in with an empty password multiple times, locking the account.

#6150, TFS111007-012964

AUTHENTICATION METHOD NOT LOGGED FOR BoKS SSH LOG ENTRIES

The authentication method used when a user logged in was not recorded in the BoKS audit log, which led to a lack of transparency and information for debugging and troubleshooting.

#6146, TFS120806-013696

VARIABLES FOR DEBUG MESSAGES OUT OF SCOPE IN ldapusersync.pl

A code problem in the ldapusersync.pl program led to a pair of variables being used out of scope.

#6136, TFS101028-012067

PARAMETERS FOR DRAINMAST PERFORMANCE MONITORING IN DOCUMENTATION

The configuration parameters for performance monitoring of the drainmast_download and drainmast_pswupdate daemons were not documented.

#6121, TFS120214-013240

SUB-OPTIMAL INACTIVITY CHECKING IN bksd

The bksd program did not check user inactivity in an optimal manner, leading to delays in taking action on inactive user sessions.

#6120, TFS090622-105729

su DUMPS CORE IN bp_verify_passwd_data

If a call to servc to get user data fails, su dumped core in the pam library bp_misc:bp_verify_passwd_data() (affected PAM platforms only).

#6119, TFS120508-013440

MULTIPLE lsbks -v HANGS IN DOMAIN WITH LARGE NUMBER OF USERS

The command "lsbks -v" stopped responding in a domain with a six- figure number of users.

#6118, TFS120508-013440

lsbks -v SLOW WITH LARGE NUMBER OF USERS

With a six-figure number of users in the domain, the "lsbks -v" command took a considerable time to complete.

#6117, TFS120314-013313

kslogs SHOULD CLOSE UPON REBOOT

Log messages were received about keystroke logs being open on the system even though there were none. This was caused by kslogs not having been cleanly closed and transferred to the Master on server reboot, causing these messages.

#6116, TFS080528-122501

KSLOG FILES SHOULD BE EXCLUDED FROM FILE MONITORING

The $BOKS_data/kslog directory and contents should be excluded from the file monitoring function as this directory only contains transient files.

#6113, TFS120511-013459

BoKS sshd MODIFIES THE PATH

When a user logged in with BoKS sshd they got a different path compared to the path when logging in with native sshd.

#6112, TFS090623-165743

BAD WARNING DURING NIS PASSWD UPDATE WITH EMPTY GROUP FILE NAME

The warning in boks_errlog when BoKS tried to update passwords in NIS and the group files field of the BoKS nismap entry was empty was misleading as it reported "WARNING: Could not read /etc/group".

This message has been updated to be more accurate.

#6108, TFS120924-013810

SPACE IN PROGRAM GROUP BREAKS SUEXEC

If a program group was defined with a trailing space character in one of the program definitions, this denied users access on any SUEXEC Access Routes including that program group.

#6105, TFS130109-013981

lsbks -v DUMPS CORE

Running the command "lsbks -v" caused a core dump when reading the group table.

#6090

debug MAY OVERFLOW INTERNAL BUFFER

Turning on debug on the BoKS Master when adding the AIX osroleset made boks_master dump core in the debug routines.

#6015, TFS130102-013971

INCOMPREHENSIBLE LOG MESSAGE FROM sshd IF $HOME/.ssh HAS WRONG PERMISSION

The error message returned when checking the writability of the authorized keys file and directories above it when StrictMode was turned on was unclear, saying only "SSH public key strict modes check failed."

#6014, TFS121008-013837

ldapsync DOES NOT HANDLE NON DES-CRYPT PSW HASHES EXCEPT SSHA

ldapsync did not cause non des-crypt password hashes to be imported correctly from LDAP to the BoKS database due to a wrongly-constructed call to modbks.

#5992, TFS120717-013655

boksinfo DOES NOT FOLLOW logadm -d /dir

boksinfo located the audit log file by checking whether $BOKS_data/ LOG existed, and did not check whether the directory had been changed using the logadm command.

#5991, TFS120416-013396

DIRECTORY PERMISSIONS WHEN USING SUEXEC

BoKS performed some checking of owner and group permissions for executables run via SUEXEC but BoKS Manager 6.7 adds enhanced permissions checking which can be set using the modifier "safepath".

See the BoKS Manager Administration Guide for more information.

#5990, TFS100511-190353

ABILITY TO SYNCHRONIZE LDAP MANUALLY WITHOUT KNOWING THE PASSWORD

This request to run an LDAP synchronization manually without knowing the password relates to the old BoKS Manager administration GUI, which is deprecated in BoKS Manager 6.7.

#5989

adsync FAILS TO UPDATE USER'S REAL NAME TO EMPTY STRING

If the GECOS / Comment field or Real Name was set in BoKS but set to an empty string in Active Directory, the adsync program did not over- write the string with an empty string in BoKS.

#5984, TFS120621-013590

LOG REPLICATION CAUSES REPLICA UPDATE DB FAILED ERROR

When replicating log data to a Replica the update failed with the following error message:

"WARNING: async db update of replica <ip-address> failed, error 101"

#5981, #6418, TFS121101-013881, TFS130327-014159

SECURITY ISSUES WITH BoKS setuid PROGRAMS

The BoKS ssh client program uses a setuid helper program named boks_gethostkey to fetch ssh public keys stored in BoKS. This program allowed debug level and debug file location to be controlled from the command line, thus making it possible for unprivileged users to overwrite system files with debug output.

Other BoKS setuid programs tcpcrypt, suexec and xdl allowed debug level but not debug file location to be specified from the command line. Although this is not necessarily insecure it may leak information not intended for unprivileged users.

All BoKS setuid programs have now been modified to only allow debug configuration by the administrator using the bdebug program.

#5966, TFS121211-013955

BoKS BRIDGE DOESN'T CLOSE BROADCAST SOCKET AFTER FORK

The BoKS receive bridge did not close the socket listening for broadcasts in forked off child processes, leading to a "FATAL ERROR: Can't bind broadcast socket, Address already in use" error.

#5956, TFS121109-013902

mkhome MAN PAGE ENHANCEMENTS

The BoKS man page for mkhome contained some inaccuracies and unclear formulations.

#5945, TFS121130-013928

httpsrv SHOULD NOT RUN ON REPLICA

It was possible to run the httpsrv program for the old Administration GUI on a Replica but the BoKS log recorded the administration as having been done on the Master. This program should not be possible to run on a Replica.

#5934, TFS120403-013368

FORMATTING PROBLEMS IN ldapsync.cfg MAN PAGE

The BoKS man page for ldapsync.cfg contained various formatting problems affecting its readability.

#5922, TFS111021-012993

BUG IN PATCH POST-INSTALL SCRIPT

The file $BOKS_etc/bokscron.conf contained duplicate entries for boks_errlog_check.

#5893, TFS120627-013609

BoKS ROOT TAR ARCHIVE CHANGES DIRECTORY PERMISSIONS

The way the BoKS ROOT tar archive was packaged meant that the directories were given permissions not appropriate to all platforms.

#5892, TFS120605-013538

FAILED UPDATES OF /etc/passwd AND /etc/shadow NOT LOGGED

Certain instances of failed updates to /etc/passwd and /etc/shadow were not logged to boks_errlog or the BoKS audit log.

#5881, TFS100412-134047

MALFORMED SUEXEC ROUTE ALLOWS EXECUTION OF ANY COMMAND

Adding an Access Route for a User Class of the format "SUEXEC:$USER@*->root@*" gave any user in that class rights to run any program as root, where it should have given no SUEXEC access at all.

#5879, TFS120823-013742

timezones MAN PAGE UPDATES REQUIRED

The man page for timezones needed an update regarding times in bkslog, server agent and replica timestamps.

#5860, TFS120906-013777

ENHANCE DESCRIPTION OF AUTO_REGISTERED

The BoKS ENV variable AUTO_REGISTERED did not have a detailed explanation of its purpose in the BoKS man page ENV.

#5823, TFS120118-013176

CONSISTENCY CHECKING IN boks_master FOR ALARM LOG COMMAND

There should be better consistency checking in boks_master of the configured alarm log specification and error logging. NOTE: The fix for this issue was already included in BoKS Manager 6.6.2, registered under the issue number #5063.

#5822, TFS120424-013420

SSH RSA HOST KEY SIZE CHANGED TO 2048

The SSH RSA host key created by BoKS setup program has been changed from 1024 bit to 2048 bit.

#5809, TFS110718-012773

lsbks DOES NOT CORRECTLY DISPLAY SOURCE OF ASSIGNED XROLES

In the output of the lsbks command, the xRoles assigned to users were not displayed separated into columns in an easily-readable manner.

#5808, #4930, TFS091013-175924, TFS100725-2510321, TFS090903-154802

hostkey -c -h DOES NOT RECOGNIZE UNDEFINED NODEKEY

The command "host -c -h <host>" printed a hash string even when the specified host did not in fact have a nodekey set in the database and an error should have been displayed instead.

#5807, TFS120227-013271

hgrpadm -d -g SHOULD FAIL IF USERS EXIST

Deleting a Host Group using the "hgrpadm -d" command should not work if the specified Host Group contains members.

#5805, TFS120302-013282

ERROR "Unknown Bridge Protocol Version" SHOULD REPORT PEER ADDRESS

The message "Unknown bridge protocol version..." report from a receive bridge in the boks_errlog file did not include the IP address of the peer generating the message, making troubleshooting impossible.

#5804, TFS120626-013604

cadm RETURNS NO OR INCONSISTENT ERROR CODE

When using the command "cadm -E" to set environment variables on a host, the program could return an incorrect 0 exit code even if the operation had not been successful.

#5748, TFS121119-013914

SUEXEC WILDCARD DESCRIPTIONS IN DOCUMENTATION

The Administration Guide incorrectly stated that it was possible to specify wildcards for TOUSER in SUEXEC Access Route definitions.

#5746, TFS111201-013084

$BOKS_etc/consoles NOT DOCUMENTED

The file $BOKS_etc/consoles, used to define device names for the console for emergency login, was not documented in the BoKS Manager Administration Guide.

#5733, TFS120723-013670

adjoin mydomain DOES NOT MAKE mydomain UPPERCASE

When you joined a host to an Active Directory, the domain name in the keytab.conf file was not converted to upper case, causing Kerberos authentication to not function correctly.

#5729, TFS120824-013744

routeadm INCORRECTLY ERASES USER CLASS ACCESS ROUTES

If routeadm was used to remove a program group from a User Class, but a non-existing program group was specified, all the Access Routes for that user class were deleted.

#5724, TFS120508-013440

lsbks MEMORY LEAKS WHEN LARGE NUMBER OF USERS LISTED

When the lsbks command was used to list a large number of users, memory leaks caused the process to grow to several gigabytes.

#5721, TFS120723-013672

adjoin join DOES NOT ENABLE "adjoin autoupdate"

When a host was joined to an Active Directory, the ADJOIN ENV variable was not set to "on", causing the machine to fail to run "adjoin update" in order to renew the its Kerberos password every 30 days.

#5714, TFS120907-013783

LISTING SLOW WITH hostprereg

The command "hostprereg -l" used to list host preregistrations in the BoKS database was slow to execute.

#5712, TFS121031-013879

FUNCTION expand_host_flg() CAUSES SYSTEM TO SLOW DOWN

The function expand_host_flg(), used by boksdiag, cadm, groupadm and mkhome, fetched information for all hosts in the database, causing the operation of these programs to slow down considerably.

#5702, TFS120809-013704

modbks -G DOES NOT WORK CORRECTLY

When changing a Host Group for a user using the command "modbks -G", password delete requests were sent directly to clients instead of batched, causing accounts not to be removed from offline clients.

Note in addition that the "modbks -G" command does not support wildcard notations for Host Group members.

#5701, TFS120817-013719

UNKNOWN USER WITH EMPTY PSW MAY CREATE INFINITE LOOP

If servc auth was called with an unknown TOUSER and an empty PSW string this could cause an infinite loop of client to servc calls.

#5700, TFS120720-013666

FAILED LOGIN COUNT DOES NOT INCREASE WITH SU / SECURID

When failed login attempts were made using a SecurID token to authenticate for SU, the failed login count did not increase.

#5699, TFS120316-013324, TFS120530-013523

MEMORY LEAK IN boks_servc

A memory leak in servc caused processes to grow and finally stop responding when they were out of memory.

#5698, TFS120514-013474

RESTART OF boks_manager CAUSES bridge_servm_s TO DUMP CORE

When the boks_manager process started up, the bridge_servm_s process could receive an empty reply from a Replica if that Replica was in the process of receiving database updates, causing it to dump core.

#5680, TFS121008-013837

servc SHOULD RECREATE ALL HASHES WHEN COMPLETING SET OF HASH FORMATS

When servc creates hashes where the set of hash formats is incomplete for imported password hashes it now recreates the hashes using the current system truncation length TAB_SYS.PSWMAXLEN rather than based on the truncation length of the existing single hash.

#5576, TFS120720-013666

FAILED LOGIN COUNT DOES NOT INCREASE WITH SU/SECURID

When a user attempts to authenticate using a SecurID token for a su operation, and the authentication fails, this does not increase the failed login count for the user.

#5446, TFS120605-013537

/etc/shadow FILE NOT UPDATED IN A SECURE WAY

A temporary file is used for a brief time when creating the /etc/shadow file that does not have appropriately secure file permissions.

#4932, TFS101005-011947

WRONG LOCATION DOCUMENTED FOR pre_mkhome AND post_mkhome

The documentation states that post_mkhome and pre_mkhome are run in the directory $BOKS_etc, bit they are actually run in $BOKS_lib.

#4921, TFS111206-013098

INSUFFICIENT INFORMATION ABOUT SUPPORTED SSH PROTOCOL VERSION

The man pages, manuals and online help do not explain clearly that the BoKS sshd daemon only accepts SSH protocol version 2 connections and does not accept version 1 connections.

#4405

man ENV TRUNCATES

When you display the man page for ENV using the command "man ENV", the output displayed is truncated at the description for the ENV variable UIDRANGE. This issue affects non-Linux platforms only, i.e. HP-UX, IBM AIX and Oracle Solaris.

TFS100725-254653, TFS100725-254704

UNABLE TO CONTROL SHELL LIMITS VIA PAM FOR SSH

boks_sshd did not control shell limits for users set via PAM configuration files. This is now possible for all platforms except HP-UX. See the section "NEW FEATURES AND CHANGED FUNCTIONALITY" for more details.

Fixed Issues on IBM AIX

#6268, TFS130225-014093

ssh -t HANGS TO boks_sshd ON AIX

Running remote commands with "ssh -t" to boks_sshd on AIX hosts resulted in ssh stopping responding.

#6153, TFS110325-012500

CORRUPT BoKS ENV FILE CAUSES SINGLE USER MODE LOGIN TO FAIL

On AIX, console login in single user mode failed if the $BOKS_etc/ENV file had become corrupt.

Fixed Issues on Red Hat

#6091

INCORRECT FILE LIST FOR xRBAC pvi

When generating the files lists for the xRBAC pvi editor (privileged editor), a processing error meant that the config file included pointers to some files that did not exist on the platform.

Fixed Issues on Red Hat 5

#5638, TFS130306-014118

BoKS PAM MODULE DOES NOT PROPERLY RESTORE SIGNAL HANDLERS

The BoKS PAM module changes some signal handlers while it is executing, but did not always restore the signal handlers when relinquishing control to the calling application. This resulted in the GDM keepalive ping causing remote sessions to crash because the expected signal handler is not in place.

Fixed Issues on Red Hat 6

#7530

INSTALL FAILS ON RED HAT 6 IF SELINUX IS NOT ENABLED

In the Revision A2 package of BoKS Manager 6.7, the install operation failed if SELinux was not enabled on the host.

Fixed Issues on Oracle Solaris

#6156, TFS120821-013729

PERFORMANCE PROBLEMS WITH BoKS sshd DAEMON ON SOLARIS SPARC

On Oracle Solaris on sparc, non-optimized code caused performance issues with the BoKS sshd daemon.

Fixed Issues on Oracle Solaris 11

#6005

INSTALLING BoKS IN A NON-GLOBAL ZONE

When installing BoKS in a non-global zone, the installation process uses the /usr/sbin/modinfo command to determine whether BoKS kernel modules have been installed in the global zone. By default the /usr/sbin/modinfo command is not available in non-global Solaris 11 zones.

Fixed Issues on SuSE Linux

#6142, TFS121004-013834

newgrp ALLOWS newgrp TO GROUP WITH NO PASSWORD EVEN IF USER NOT MEMBER

The newgrp function on SuSE Linux allowed a user to newgrp to a group even if the user was not a member of that group if the group had an empty password. To prevent this, BoKS no longer creates groups with empty passwords.

Fixed Issues on VMWare 4.0-4.1

#4376, #4379

CONFIGURATION FOR vpxuser ACCOUNT NOT SET UP CORRECTLY

Installation on VMware 4.0-4.1 fails to set up the correct PAM configuration for the "vpxuser" user account. Install hotfix HFBM-0001 to correct this issue.

Go to top

Known Issues

Issues identified in this release, with workarounds where appropriate.

NOTE: The addition of support for non-crypt Unix password hashes makes it possible to use longer password lengths than 8 characters. However, be aware that different services may impose limits on password length that are outside the control of BoKS Manager. For more details, see the Administration Guide.

Known Issues on All Platforms

ABOUT UID AND GID RANGE IN BoKS

Valid range for uid and gid differs for different platforms. Uid and gid can also be signed or unsigned depending on platform. BoKS stores uid and gid internally as signed 32-bit integers, thus supporting a range of -2147483648 to 2147483647.

On platforms using unsigned uid/gid, boks_clntd converts signed to unsigned and vice versa when writing uid and gid from/to the local system files. For example, on AIX the nobody account can have both uid and gid 4294967294. When reading the /etc/passwd file with cadm the uid and gid are converted to the corresponding signed 32-bit integer -2

BoKS # cadm -l -f passwd -h aix71 | grep nobody

nobody:*:-2:-2::/:

Similarly to creating an account with a uid/gid larger than 2147483647 on the local system the uid/gid value in BoKS should be set to the corresponding (negative) 32-bit signed value. In BoKS a uid of -1 will result in local unsigned uid of 4294967295 etc.

Note also that the valid uid/gid range on some platforms is less than the full range of a 32-bit integer.

The BoKS ENV variable UIDRANGE can be used to limit the range of uid/gid values accepted by BoKS.

#8205

ENV VAR PORT_RANGE CAUSES FATAL ERROR

The ENV variable PORT_RANGE, when set, causes the boks_bridge process to exit and write the following error to the BoKS error log:

```
FATAL ERROR: ENV:PORT_RANGE Incorrect, Success (0)
```

This variable should not be used.

#6580, TFS120606-013543

USERS IMPORTED WITH WRONG UID / GID

This issue occurs if you are importing users from a host running a 64-bit Linux Operating System and you select either the option to import from the “NIS passwd map” or “NIS maps and /etc/passwd file”, (which use the `read passwd` argument to `boks_clntd`). For users with a uid or gid greater than 32767, this uid/gid is interpreted as a negative number, meaning the wrong uid/gid is written to `/etc/passwd` and/or `/etc/group` on the host or Host Group you are importing to.

#6480

CANNOT REGISTER ecdsa HOST KEYS IN PRE-6.7 DATABASE

The field SSHHOSTKEYTYPE is too short to store ecdsa SSH host keys in pre-6.7 BoKS databases. Therefore is it not supported to register ecdsa host keys for Server Agents running BoKS 6.7 if the Master and Replicas are running a BoKS version pre-6.7.

#6436

USER LOGON NAME REQUIREMENTS FOR AD BRIDGE PASSWORD SYNCH

For password synchronization to function correctly between Active Directory and BoKS, the "User logon name" and "User logon name (Pre-Windows 2000)" must be identical for a user, and the "User Logon Name (Pre-Windows 2000)" must contain only ASCII characters.

#6265, TFS130204-014042

INCORRECT MESSAGE FROM FILMON

If a file being monitored by BoKS file monitoring is removed during a scan, but recreated when filmon processes the old database to discover e.g. files that have been removed, filmon incorrectly reports that the actual monitoring configuration has changed and the file in question is no longer being monitored.

#6127, TFS110706-012754

BoKS FILE MONITORING ISSUES

This report includes two issues where BoKS file monitoring does not function as expected:

1. If a "top level" directory or file which is specified in the file monitoring configuration file is missing on the host, filmon fails with an error rather than logging the discrepancy and continuing with the scan.

2. If a "sub level" file or directory is missing, filmon returns the same error message but continues scanning without, however, logging the discrepancy.

#6123, TFS120809-013704

LIMITATIONS IN modbks -G FUNCTIONALITY

The command modbks -G, used to change the Host Group part of a user account, has some limitations including lack of support for wildcard members added to Host Groups and lack of support to handle users with the same login name in different Host Groups.

#6115, TFS090821-141531, TFS100725-2510213

BROKEN DNS ENTRY CAUSES ACCESS ROUTES NOT TO FUNCTION

If a host has a broken DNS entry, so that its IP address can be mapped to a name, but the name cannot be mapped back to an IP address, Access Routes to the host that contain an IP address definition do not function correctly even if the variable HOSTUNKNOWNADDRESSOK is set to "on", in which case it might be expected that the Access Route would treat the host as an unknown host.

#6114, TFS120510-013451

FULL DISK CAN CAUSE CORRUPTED ENV FILE

In the event of a disk becoming full on a running system, certain operations can cause the BoKS ENV file to become corrupted, for example bdebug and BoKS activation / deactivation operations.

#5750, TFS120723-013671

adjoin DOES NOT DETECT IF HOST ALREADY JOINED TO KERBEROS SERVER

It is possible to join a host to an additional Active Directory even when it is already joined to another Kerberos server. This should be avoided as it could lead to unforeseen authentication behavior and is not a supported configuration.

#061017-112910

PAM-BASED X-LOGIN ACCESS CONTROL MAY FAIL ON FIRST LOGIN ATTEMPT AFTER BoKS ACTIVATION/DEACTIVATION

PAM-based X-login using dtlogin/gdm/kdm/xdm is locked to a PAM configuration when displaying the login dialog and waiting for a login attempt.

When BoKS is activated/deactivated the changed PAM configuration does not take effect until AFTER the first login attempt following a BoKS activation/deactivation. On the first login attempt after activation/deactivation the login may fail with an error message, or the user may be allowed to log in even if access should NOT be allowed according to BoKS access control rules. Affected platforms are IBM AIX 6.1 & 7.1, Red Hat Linux, SuSE Linux and Oracle Solaris.

WORKAROUND: To avoid this issue, FoxT recommends always restarting the X Windows system after you activate or deactivate BoKS protection.

#5120

'CANNOT READ KEYTAB FILE' ERROR WITH SSH KERBEROS AUTHENTICATION

ssh login with Kerberos authentication fails and the boks_errlog file contains the message "cannot read keytab file".

WORKAROUND: This error can be avoided by ensuring that the server uses the Fully-Qualified Domain Name as hostname. If the server uses a shorter version of the hostname, the OpenSSH daemon does not find the local key in the keytab file, since this is named after the FQDN.

#4876, TFS110420-012573

INTERPRETATION OF WILD CARDS IN PROGRAM GROUP DEFINITION

The man page for the pgrpadmin program does not state if / how wild cards and regular expressions can be used. Wild cards are allowed with pgrpadmin (* and ?), but not regular expressions (e.g. [a-z]).

#060825-163100

RLOGIN WITH SAFEWORD GENERATES "PAM AUTHENTICATION FAILED" MESSAGE

When a user performs rlogin and authenticates using a SafeWord token on Linux platforms, "PAM authentication failed" messages are written to /var/log/messages, even though the authentication is successful in BoKS.

NON-CRYPT PASSWORD HASHING MAY REQUIRE ADDITIONAL OS SOFTWARE

Use of non-crypt password hash formats might require installation of additional system software packages or fixes on Oracle Solaris and IBM AIX.

See the section "Unix/Linux Password Encryption" in the BoKS Manager Administration Guide for details.

GROUP PASSWORDS ARE NOT SUPPORTED

Before installing BoKS any existing group passwords must be removed from the /etc/group file. If shadowed group passwords are in use i.e. an /etc/gshadow file exist, the entire /etc/gshadow file should be removed.

#061023-132719

BoKS DOES NOT START PROPERLY IF INSTALLED WITH A VERY LONG PATH

The BoKS base install paths (that have the default settings /opt/boksm, /etc/opt/boksm and /var/opt/boksm) should not be set to a path that is longer than 128 characters.

TFS050425-101718.1

TELNET SSL-PROXY REQUIRES WORKING SERVICE NAME MAPPING

During BoKS setup, the $BOKS_lib/proxyinst script installs the telnet ssl-proxy daemon used for SSL encrypted telnet sessions from BoKS Desktops to BoKS hosts, and adds it to the local /etc/services file with the service name mapping

```
telnets    992/tcp
```

However, if the host is configured to use an external network information service such as NIS instead of the local /etc/services file, the proxyinst script may fail.

Workaround:

If the system is configured to NOT use the /etc/services file, add the mapping

```
telnets    992/tcp
```

to the external network information database before installing BoKS. Alternatively, after installing BoKS, update the external network information database with "telnets", then manually run the $BOKS_lib/proxyinst script.

#5586, TFS120514-013475

HOSTNAME MAPPING TO EXTERNAL NETWORK ADDRESS MUST EXIST PRIOR TO BOKS INSTALLATION

RedHat Linux by default maps the hostname to the loopback address 127.0.0.1 in the /etc/hosts file at installation even if an external network address is configured for the machine.

Similarly, SuSE Linux can append 127.0.0.2 to /etc/hosts for the hostname.

For BoKS to be installed correctly, the /etc/hosts file must map the external network address to the hostname registered on the BoKS Master and the loopback address 127.0.0.1 or .2 must NOT be mapped to the hostname registered in BoKS. Before installing BoKS, check the /etc/hosts file and correct it if necessary to meet this requirement.

#6542

gunzip ERROR MESSAGE WHEN RUNNING UPGRADE

When you run boks_upgrade setup for the first time, the following error may be displayed:

```
gunzip: is.gz: No such file or directory
```

gunzip: /bin/gunzip: not in gzip format

This error can be safely ignored, as the upgrade procedure continues even though the error is displayed.

#4043

OLD SAFEWORD SERVERS MAY NOT WORK WITH OpenSSL TLSv1 PROTOCOL

The new OpenSSL version in BoKS manager 6.6.1 and later adds new extensions to the TLSv1 protocol. Old Safeword servers might not handle TLS extension negotiation correctly. To overcome this problem, a new configuration variable has been added to the BOKS_etc/safeword.cfg file named SSL_PROTO. The default value is "TLSv1" but the value can be set to "SSLv3" to make Safeword authentication work with old Safeword servers.

TFS041014-155307

FILES MUST BE TRANSFERRED MANUALLY AFTER UPGRADING REPLICA

After you upgrade a Replica, or reinstall BoKS Manager on a Replica for any other reason, you must manually transfer a number of files to the Replica by running the following command on the Master:

BoKS# push_files <replica_name>

This ensures that the Replica has all the required files in the event that it must be converted to a Master. For details, see the BoKS man page push_files.

TFS070921-083246

boks_upgrade HOTFIX INSTALL CANNOT DISTINGUISH PATCH LEVEL ON TARGET HOSTS

When installing hotfixes remotely with boks_upgrade it is not possible to limit the installation to only hosts running a specific BoKS patch level. For example, if a hotfix intended for BoKS version 6.5.1 is installed using boks_upgrade and the target is a Host Group containing both 6.5.1 and 6.5.2 hosts, the boks_upgrade program will try to install the hotfix on all the hosts in the Host Group.

Known Issues on IBM AIX

#6209, TFS121023-013865

/etc/passwd NOT UPDATED CORRECTLY ON AIX

If one creates a Unix user in BoKS without assigning a password, no stanza is created for the user in /etc/security/passwd. This causes a problem with the "pwdck" command on the clients.

#6152, TFS111103-013025

UNLOGGED LOGIN FAILURE WITH SSH

On AIX, if a user has a gid that is not present in /etc/group (or NIS), SSH to the machine may fail without an audit log in BoKS.

#6147

NATIVE SSH DOES NOT FUNCTION WHEN BoKS PROTECTION ACTIVE

When BoKS protection is active on an AIX host, the native system SSH implementation does not function correctly and should not be used.

#6151, TFS110225-012418

umask DOES NOT WORK WHEN USER SHELL SET TO /bin/false

When a user's shell is set to /bin/false, the umask value set does not function correctly in AIX 6.1 and 7.1.

OS Role Assignments Deletion

When uninstalling BoKS from a host existing local OS role assignments are not automatically deleted from the host. This may lead to unintentional exposure of the default AIX system roles isso, sa and so (boksadm and boksop OS role definitions are removed by uninstall and thus become invalid).

Workaround:

Alt 1. Before uninstalling BoKS make sure all user association to isso, sa and so for the host are removed using the BoKS Master console.

Alt 2. After uninstalling BoKS run lsuser -a roles ALL to view any existing user OS role assignment and chuser roles= <user> to remove assigned OS roles from a user.

Known Issues on IBM AIX 6.1

Use of AIX 6.1 xRBAC functionality requires installing fix pack "6100 TL1" to add 'Assign Roles to a User' functionality.

For details, see:

- https://www-304.ibm.com/support/docview.wss?uid=isg1fixinfo107339

Known Issues on HP-UX

#4354

BoKS PASSWD DOES NOT UPDATE SHADOW USING NEW CRYPT

When configuring HP-UX to use SHA512 passwords using CRYPT_DEFAULT and CRYPT_ALGORITHMS_DEPRECATE in /etc/default/security, it is important not to have any whitespace characters after the values to these parameters. While HP-UX accepts this, BoKS currently does not.

TFS100106-110037

HOST/NODE NAME LENGTH RESTRICTION ON HPUX

By default, the nodename is limited to 8 bytes on HPUX 11. BoKS requires that the nodename and short hostname (hostname without domain component) are identical and at most 8 bytes long.

Tuning the kernel to support longer node/host names using the expanded_node_host_name kernel parameter is not supported by BoKS.

TFS070927-143037

UNINSTALL MAY NOT REMOVE SOME FILES

When you uninstall BoKS on a host running HP-UX, files for any programs that are in use, for example programs in use by logged in users, cannot be removed.

WORKAROUND: Move the top directory (/opt/boksm) to another name then try to remove it later when users have logged out and programs are no longer in use.

Known Issues on HP-UX 11iv2 & 11iv3

#4357

HP-UX 11iv2, 11iv3 AND SHA512 PASSWORD LENGTH

With only the patch to support SHA512 hashed passwords installed on HP-UX 11iv2 and HP-UX 11iv3, the system supports passwords of a maximum 8 characters in length. If you configure BoKS to use longer passwords, you will not be able to log in when BoKS protection is deactivated or BoKS is uninstalled. For HP-UX 11iv3 a separate HP-UX patch is available to support longer passwords with SHA512 hashed passwords.

Known Issues on Red Hat

DISABLE SELINUX BEFORE INSTALLING BoKS MANAGER

Red Hat Linux 5, 6 and 7 includes SELinux. BoKS Manager does not function properly with SELinux enabled. SELinux must be disabled before you install BoKS Manager.

WORKAROUND ON RED HAT 6 / 7

A separate RPM is available - for Red Hat Linux 6 and 7 - that includes an SELinux policy that enables BoKS Manager to function correctly with SELinux activated. The RPM is available for download from the FoxT Customer Service website, and is named `boks-selinux-X.X-X.elY.noarch.rpm`, where `X.X-X` is the current version of the policy, and `Y` is the RedHat release number.

Once you have installed the RPM, you must apply hotfixes `H FBM -0164` and `H FBM -0167` to enable BoKS to support the SELinux policy. For details of the scope of the hotfix, see the hotfix READMEs.

Note that if you have previously applied hotfix `H FBM -0038` to add support for SELinux, this hotfix must be uninstalled before you apply hotfix `H FBM -0167`.

Known Issues on Red Hat 7

#7593

journalctl SHOWS 'TOO MANY LOGIN TRIES (1)' WHEN LOGIN FAILS

If a user gives the wrong password when attempting to log in using rlogin, the log shown by journalctl incorrectly shows the message "`TOO MANY LOGIN TRIES (1) FROM ... FOR ..., Have exhausted maximum number of retries`".

The BoKS audit log shows the correct error (wrong password).

Known Issues on Red Hat 6 and 7

#7612

LOGIN CAUSES AVC ABOUT .boks_uenv FILE

When SELinux is enabled, a user's `.boks_uenv` file is not read when the user logs in using rlogin, rsh, rexec or telnet.

#7611

suexec WITH SECURID FAILS CAUSING SELINUX AVC ERROR

suexec using SecurID authentication does not work on Red Hat 6 and 7 when SELinux is enabled.

#7605

SELINUX DOES NOT PERMIT chroot

BoKS sshd on Red Hat 6 and Red Hat 7 does not work with chroot when SELinux is enabled.

#7596

BLOWFISH PASSWORD HASH ALG NOT SUPPORTED

Even though RedHat supports the Blowfish algorithm for password hashing, the BoKS RedHat 6 and RedHat 7 ports do not. As an alternative, you can use for example the AES password hash algorithm instead.

#7594

EXTRA SELINUX ENV VARS MISSING WHEN USING boks_sshd

On RedHat 7 and RedHat 6, the environment variables `SELINUX_ROLE_REQUESTED`, `SELINUX_USE_CURRENT_RANGE`, and `SELINUX_LEVEL_REQUESTED` present when logging in using the system sshd with SELinux enabled are not present when logging via the BoKS `sshd`.

Known Issues on Red Hat 6

CANNOT CHANGE PASSWORD HASH ALGORITHM CONFIGURATION WHEN BoKS IS ACTIVE

On Redhat Enterprise Linux 6, the password hash algorithm configuration can be changed via the utility /usr/bin/system-config-authentication. Changing the password hash algorithm configuration updates the parameter "crypt_style" in file /etc/libuser.conf, see libuser.conf(5) and the password hash option to the pam_unix.so modules in /etc/pam.d/system-auth-ac, see pam_unix(8).

When BoKS protection is active, /etc/pam.d/system-auth-ac is a soft- link to /etc/pam.d..org/system-auth-ac and this apparently prevents /usr/bin/system-config-authentication from updating the password hash option of the pam_unix.so module.

Although the pam_unix module is not used for authentication when BoKS protection is active, it is important that the password hash option is correctly configured because this configuration is also used by BoKS to select hash algorithm when provisioning user accounts to the machine.

WORKAROUNDS:

ALT 1. Deactivate BoKS protection before changing the password hash algorithm with /usr/bin/system-config-authentication.

ALT 2. Edit the password hash algorithm configuration manually using a text editor in the files /etc/libuser.conf and /etc/pam.d/system- auth-ac.

Known Issues on Oracle Solaris 11

#6423

DUPLICATED LOGIN MESSAGE AT SSH LOGIN TO SOLARIS 11

When you log in to a BoKS host running Oracle Solaris 11 using SSH, the login message may be displayed twice.

WORKAROUND: Set the parameter PrintMotd in the sshd_config file to "no", which prevents ssh from printing the motd file.

#5757

BROKEN PAM IMPLEMENTATION IN SOLARIS 11 proftpd

The Solaris 11 ftp service uses proftpd which has a broken PAM implementation. After a successful authentication the proftpd calls pam_open_session and then immediately pam_close_session although the user session is still open.

BoKS uses the PAM open/close session calls to generate login/logout log messages for the BoKS audit log and the result is that at both BoKS login and logout, log messages are set at ftp session start.

#5736

ONLY inetd SERVICES SUPPORTED FOR sysreplace ACTIVATED/DEACTIVATED SERVICES

Activating/deactivating services at BoKS activation/deactivation using the BoKS ENV variables SYSREPLACE_ACTIVATED_SERVICES and SYSREPLACE_DEACTIVATED_SERVICES is only supported for services managed by inetd. Specifically the ftp services is not managed by inetd in Solaris 11 and is not supported by the sysreplace activated/deactivated services function.

Go to top

Known Issues on Debian 7 / Ubuntu 12

Note that while both Debian 7 and Ubuntu 12 both support ftpd and vsftpd for authentication, if you want to make use of the `SYSREPLACE_ACTIVATED_SERVICES` and `SYSREPLACE_DEACTIVATED_SERVICES` configuration variables for ftp (for advanced BoKS Protection configuration), only vsftpd works for Debian and only ftpd works for Ubuntu.

#7697

DEBIAN & UBUNTU VERSIONS ASSUME DEFAULT inetd IS USED

Although on Debian and Ubuntu you can select which inetd daemon to use, for example you can use xinetd instead of the standard default openbsd-inetd, the BoKS Manager 6.7 version built for these platforms only works with the system default openbsd-inetd. If you have configured the system to use any other daemon, BoKS does not function correctly.

#7656

nslookup RUN IN BoKS SHELL GIVES ERROR REGARDING libcrypto.so

When in the BoKS shell, nslookup (and possibly other commands) fail, returning an error stating that `$BOKS_lib/shlib/licrypto.so.1.0.0 has no version information` available. This issue is caused by an incompatibility between the BoKS and system version of the libcrypto.so shared library. In the BoKS shell, the BoKS version of the library is found first.

WORKAROUND: Either exit the BoKS shell, or temporarily unset `LD_LIBRARY_PATH` when running the command , e.g.:

```
BoKS # LD_LIBRARY_PATH= nslookup
```

#7657

STANDARD SYSTEM SCREENLOCK DOES NOT PROMPT FOR SECURITY PIN

The standard screensaver (gnome screensaver) runs as the user logged in, and so cannot determine how the user authenticated when logging in, so will ask for password to unlock the screen even if e.g. an RSA SecurID token was used to log in.

WORKAROUND: Configure the system to use the BoKS screenlock program `xdl`, which is located in the directory `$BOKS_bin/X11`.

Known Issues on Ubuntu 12

#7658

PROMPTING AND TEXT DISPLAY ISSUES WITH X LOGIN ON UBUNTU

When logging in using X (unity) on Ubuntu, a user is normally always selected and a prompt is displayed requesting e.g. password. If the authentication method for that user changes, this is not reflected in the prompt.

WORKAROUND: Select another user, then the first user again.

In addition, text messages from BoKS are truncated and shown for a very short time.

WORKAROUND: There is no workaround to this issue. This is caused by a limitation in the Ubuntu X-login client.

Getting Support And Service

If you have a question about a specific item in this document, refer to the case number or title listed at the start of the item when you place your technical support call.

- Fox Technologies, company, products and sales ~ http://www.helpsystems.com
- Technical support login ~ Portal login via https://community.hepsystems.com