

Access Controls for Servers

BoKS Access Control for Servers protects a
UNIX/Linux server network

A FoxT White Paper
03.19.2008

About the FoxT Solutions

FoxT solutions provide identity and access management, security with strong authentication and time-saving, simplified administration:

- BoKS Access Control for Servers (UNIX/Linux servers)
- BoKS Access Control for Applications
- BoKS Access Control for Workstations

FoxT solutions enhance existing Identity and Access Management infrastructure. Features that can be integrated include centralized user administration, centralized policy management, centralized audit logging, access control with strong authentication, single sign-on, encrypted communication, file encryption, credential management and secure messaging.

● Introduction to BoKS Access Control for Servers

BoKS Access Control for Servers is a comprehensive management solution for large enterprises whose networks include multi-vendor UNIX or Linux platforms. BoKS Access Control for Servers is designed to meet the administrative and security needs of financial institutions, government organizations and global corporations who operate in dynamic, diverse and security-sensitive environments.

Fox Server Control has a small footprint on the managed UNIX and Linux systems and does not affect the operating system kernel. It can be installed in a heterogeneous UNIX environment to provide added value while all the native UNIX features remain unaltered.

Primary components are a BoKS Manager server that maintains a central security database, Replication servers for backup and failover, and client packages installed and remotely maintained on each UNIX/Linux server.

Configuration, maintenance and daily administration are highly customizable through a flexible, modular command line interface as well as a user-friendly graphical user interface. Management of users, credentials, hosts, access rights, logs, backups and so on are all delegable to individual administrators with configured rights. Administrators can run under their own identities and credentials, thus protecting root account passwords and limiting root passwords to a limited number of individuals. Support for major two-factor and strong authentication technologies and corresponding third-party hardware and software allows direct out-of-the-box installation of a BoKS Access Control for Servers solution that dovetails with existing infrastructure.

BoKS Access Control for Servers customers include prominent worldwide banks, large hospitals, tax authorities, police systems, and major industrial corporations, as well as medium-sized businesses with intensive computing services to be managed and protected.

Key Values

BoKS Access Control for Servers enhances existing network infrastructure by providing:

- Centrally managed access control for over-the-network services such as telnet, SSH and ftp. Only configured access is allowed.
- UNIX to UNIX single sign-on
- Control of privileged accounts
- Enforcement of a common password policy across the domain on diverse platforms
- Auditing of all network login, access and administration to meet auditor requirements
- Centralized user provisioning and management that saves time and eases

upkeep

- Secure, encrypted access with SSH and telnet, enforceable for specified hosts and users
- Strong authentication with public key technology and two-factor devices such as tokens
- Keystroke logging of user activity for sensitive operations

By integrating with existing systems, BoKS Access Control for Servers leverages invested capital and administrative effort. Ongoing design and development at FoxT integrates the latest technology, new requirements, support for major third party systems and latest OS releases from UNIX/Linux vendors.

Supported Environments

When BoKS Access Control for Servers products are ported to a particular UNIX/Linux brand, they are adapted for user administration to the standard features existing on that platform. Each platform can run with its own technology and conventions, using BoKS Access Control for Servers as the gateway to a central, standardized data repository.

BoKS Access Control for Servers solution is available for all the common UNIX and Linux brands including among others the following systems:

- HP HP-UX
- IBM AIX
- RedHat Enterprise Linux
- SCO UnixWare
- Silicon Graphics Irix
- Sun Solaris
- SuSE Linux

BoKS Access Control for Servers also supports commonly used virtual operating systems such as VMWare, IBM VIO and zLinux that allow organizations to consolidate server assets.

See www.foxt.com for details on current platform support.

● BoKS Access Control for Servers Core Functionality

The BoKS Access Control for Servers solution is modular, extensive, scriptable, extremely flexible and designed for easy customizing to meet customer requirements. The solution's functionality falls broadly into the following areas:

- Identity Management
- Access Control and Server Protection
- Auditing
- System performance and reliability

Identity Management

Centralized user administration for UNIX/Linux server estates

The BoKS Access Control for Servers security database is a central repository for user accounts, credentials, access rules, encryption keys, host identities and related data within the managed network. This is the foundation for simplified management of diverse platforms across the network.

BoKS Access Control for Servers simplifies user administration in a UNIX estate by handling the creation, modification, and removal of users on thousands of machines running different UNIX or Linux brands. Password and /etc/group synchronization are pushed out automatically. A new user account can be provided across the network within minutes, and a user can likewise be removed or blocked from all access centrally and immediately.

To make managing user attributes and access rights easier, you can group users in User Classes, meaning new users can quickly inherit the privileges they need to start working. User can be added to several User Classes if needed.

To make distribution of accounts to servers easy, BoKS Access Control for Servers lets you group hosts into Host Groups which share the same user accounts and access needs.

- **Provisioning existing users** – BoKS Access Control for Servers can import users from existing password files, TCB (trusted computer base), YP/NIS, NIS/NIS+, and databases that support LDAP communication. This makes it easy to begin using the product in an existing infrastructure. It also simplifies consolidating user populations as organizations change, merge and expand.
- **LDAP synchronization of user data** – BoKS Access Control for Servers can perform automatic periodical and manual synchronization of user data in databases supporting the LDAP protocol. For organizations with LDAP directories (or planning on using one), synchronization means simple integration of BoKS Access Control for Servers enhancements with the existing infrastructure.

Strong, Configurable Authentication

Authentication of users is highly flexible and configurable on a user, host and service basis. BoKS Access Control for Servers supports strong and two-factor authentication with physical devices such as RSA SecurID® tokens and SafeWord tokens, with authentication servers such as an LDAP server, and with public key technology such as certificates and the keys used in SSH. For platforms that use PAM, BoKS Access Control for Servers can be configured either to enhance the native PAM with FoxT features, or to disable PAM and handle authentication solely with BoKS Access Control for Servers mechanisms and logic.

“We don’t manage specific compliance efforts at the corporate level. Business managers are responsible for identifying and addressing risks. We only ask them to inform us about control issues they’ve identified. But we don’t track their actions... we rely on audit tests to confirm we’re ok.”

Global Risk Manager, Top 25 Financial Institution

CA and Certificates

BoKS Manager, the central component in a BoKS Access Control for Servers solution, contains a fully functional Certificate Authority that allows an organization to issue certificates. In a BoKS Access Control for Servers solution, such certificates are used for host identification and optionally for GUI login by administrators. In a BoKS Access Control for Workstations solution, certificates are also used for user authentication during login to the workstation, and for access to UNIX/Linux servers from workstations via SSH.

Access Control and Server Protection

Centralized Access Control by Positive Configuration Only

BoKS Access Control for Servers empowers you to centrally control access using rules (termed Access Routes) that you set up in the security database. These rules enable you to specify in detail what user or User Class can access what host or Host Group using what service (telnet, SSH, etc.) on what days of week and times of day. A user can be assigned multiple routes via their User Classes and individual "single-user" Access Routes, allowing great flexibility in tailoring allowed access to each individual's needs and no more.

BoKS Access Control for Servers enhances native UNIX/Linux security, it does not replace it, so a user must still have an account on the target host, and file access rights to any programs or files that they use. BoKS Access Control for Servers makes this easy by automatically pushing out the user account and `/etc/group` data to all the hosts to which a user belongs.

UNIX to UNIX Single Sign-on

BoKS Access Control for Servers provides secure single sign-on for UNIX to UNIX via Secure Shell and telnet. With BoKS Access Control for Servers, the secure method SSH becomes even stronger and more manageable by requiring Access Routes and by allowing configured authentication methods. With BoKS Access Control for Servers, telnet can be made both encrypted and single-sign-on. When BoKS Access Control for Workstations is also installed, encrypted, single-sign-on telnet and SSH can also be provided from a workstation to a UNIX/Linux server.

BoKS Access Control for Servers also strengthens the methods rsh, rexec and rlogin so that the open UNIX/Linux environment can be kept open without compromising security. BoKS Access Control for Servers provides administrators with direct, centralized control of Access Routes and bypasses the `.rhosts` files in user home directories. The methods rsh, rlogin and rexec are often shut down due to security risk—BoKS Access Control for Servers makes them usable again by requiring a positive Access Route configuration that is easily managed and auditable.

With any of these methods, users can authenticate once at the boundary of a Host Group, then gain access to the other hosts in the group without further logging in, a convenience for ordinary users and a real time-saver for administrators.

Privileged Account Protection

BoKS Access Control for Servers includes various means that may be used individually or combined to protect privileged (for example root) accounts without having to implement complex routines that hamper your business processes. Prominent among them are:

- Administration is done under the administrator's own account
- User can use his or her own token when SUIing to root
- Separate Access Routes are required for SU
- Secure Shell's privilege separation
- A *suexec* function allowing a user or User Class to execute specific programs as another user, typically a privileged user such as root, that can also be optionally keystroke logged.

The *suexec* execute as another user function also enables you to:

- Control which specific command arguments the user can run as another user
- Group commands to simplify provisioning what programs can be executed as another user
- Allow a user to authenticate once and run multiple *suexec* commands over a configurable session time
- Allow users to execute commands as another user in the other user's environment.

These features drastically reduce the need to distribute root passwords, which only need to be known by a limited group of administrators.

Further, all user administration and Help Desk functions (unlocking terminals, resetting passwords, etc.) can be done through the BoKS Manager GUI by delegated Sub-Administrators who log in with their own accounts using the authentication mechanism that is specified for them (can be set to certificate, token or password).

Timeout

BoKS Access Control for Servers provides simplified management and uniform enforcement of timeout with its central timeout functionality for UNIX and Linux users. The user can be logged out or have screen activity locked (locking only on XDM, dtlogin and Solaris vt100-compatible terminals).

Blocking users

BoKS Access Control for Servers provides multiple user blocking mechanisms:

- *Automatic account blocking.* BoKS Access Control for Servers blocks the user after an administrator-defined number of failed login attempts. Unblocking requires administrator action.
- *Manual account blocking.* The administrator can manually block a specific user's access to the entire network protected by BoKS Access Control for Servers. This functionality is particularly useful when a user is on temporary leave or has not yet begun his or her employment.

Managed SSH

BoKS Access Control for Servers includes a complete SSH system on each server installation. Authentication methods include SSH's Public Key and Hostbased as well as BoKS Access Control for Servers passwords, tokens and certificates. The BoKS Access Control for Servers implementation includes Privilege Separation and granular access control for separate SSH services. The inherently secure SSH is strengthened by the addition of BoKS Access Control for Servers Access Routes that are mandatory and provide central control of all access. For added security on SSH Access Routes, you can specify a chroot that limits users to one specific part of the server.

BoKS Access Control for Servers simplifies Hostbased Authentication and enhances domain security by automatically distributing host public keys to protected hosts in the domain, thereby making it a realistic concept even in large networks with thousands of machines. This also makes it centrally manageable and auditable, eliminating the inherent difficulties in setup, audit and enforcement of a peer-to-peer based system. Furthermore, since only users with valid Access Routes have access to BoKS Access Control for Servers protected hosts, you centrally control which users have access to a particular host. With BoKS Access Control for Servers, Hostbased SSH becomes a centrally managed, user specific, UNIX single sign-on service.

Secure, Encrypted Communication

BoKS Access Control for Servers gives you several means of providing encrypted VPN channels to and between UNIX/Linux hosts. You can enforce the use of encrypted channels between specified hosts or Host Groups, both inside and between BoKS Access Control for Servers domains. Currently supported are SSH services and encrypted telnet.

Auditing and Security Policy

Built-In Enforcement of Security Policy

BoKS Access Control for Servers lets you define a security policy and adhere strictly to it using:

- Access Routes with type of service and other granularity, required for each access.
- User Classes that allow assigning Access Routes to users simply and manageably.
- Host Groups that simplify specifying allowable hosts in an Access Route, as well as automatically create the necessary user accounts on the hosts in the group.
- Timeout monitoring that is configurable system-wide as well as separately for individual users and for the root account.
- Blocking users that ensures immediate response to personnel changes or intrusions.
- Centralized user administration that makes system-wide removal of an account almost instantaneous.
- User account lifetime, after which the account is automatically disabled, that is useful for temporary employees, consultants and visitors.

BoKS Access Control for Servers enforces the configured policy strictly, yet is manageable within a typical dynamic environment that includes new employees, organizational changes, etc.

Password Policy

With BoKS Access Control for Servers, you define a password policy that Server Control enforces centrally each time a user changes password locally using their ordinary passwd program. BoKS Access Control for Servers provides rules for password format, expiration period, grace period, lifetime and history, as well as a dictionary of 'non-allowed-passwords'. You can also specify powerful rules for passwords using regular expressions.

Centralized Audit Trails

BoKS Access Control for Servers logs all security-related events to a central log file. Tools are available in the command line and the GUI to extract and present the log. Logs can be easily exported to a text format that allows analysis by third-party log tools. BoKS Access Control for Servers has a fully-configurable alarm log with the capability to trigger events.

Keystroke Logging

BoKS Access Control for Servers includes the capability to log user keystrokes and screen output for specified user operations and even entire sessions. This

feature provides a secure, forensic-level audit trail of exactly what administrators have done, and can be queried using a powerful search engine that includes regular expression queries.

Delegated Administration

System administrators use a Graphical User Interface (GUI) or a Command Line Interface (CLI) to manage the security database. Rights to work in the GUI can be limited to specific menus and tasks, and to groups of users and hosts, thereby allowing areas of responsibility and providing accountability. Every action in the CLI and every change in the database is logged, making every administrator accountable.

Remote Administration

BoKS Access Control for Servers supports encrypted remote administration using a browser with SSL together with a smart card, virtual card, or RSA SecurID token for administrator authentication. Remote administration can be restricted to specific hosts within or outside the domain. Remote administration is always restricted to specified administrators and always logged.

Monitoring files and directories

BoKS Access Control for Servers includes a monitoring function that surveys files and directories for changes in checksum and/or other file attributes, to detect when someone has tampered with them. An alarm log is sent if such an event occurs. Configuration is flexible and simple, making it adaptable to specific requirements.

Integrity checks

The BoKS Access Control for Servers integrity check scans the system for vulnerabilities in important system services and files and reports suspicious file permissions, ownership, content and daemon or service configurations. Integrity Checks are configured to run on a host or Host Group basis at specified intervals and can also be run on-demand.

Backup and restore

BoKS Access Control for Servers backs up and restores the database and all security-related files simply and easily. Files can be added to the save list and other configuration modified as desired. As with all functionality, backup/restore can be run directly from the command line or in scripts.

System Performance and Reliability

Scalability

In addition to the central BoKS Manager Master server, BoKS Access Control

for Servers uses Replica servers that each hold a read-only copy of the security database. These Replicas can be placed on subnets to balance loads and to provide fast, failover access across the managed network. The BoKS Access Control for Servers solution can also be implemented with separate, multiple BoKS domains for scaling, security or other purposes.

Reliability

BoKS Access Control for Servers is designed for continuous 24x7 operation. Replicas are the primary mechanism to insure that a user request for access is answered quickly and unfailingly. Each client in the domain, i.e. a machine installed with BoKS Client, BoKS Desktop, or BoKS Agent, can be configured to query multiple Master and/or Replica servers, so that it always is served. When the Master is down for a short time, Replicas can handle the basic operation of the domain, with the only limitation being that passwords and other data in the database cannot be changed. If the Master server is down for a relatively long period, any Replica server can be promoted to Master.

In the case of network problems which prevent a BoKS Client from contacting any BoKS server, authentication to specific services on the Client can still be handled by means of a configurable offline mode feature. When the servers come back on line, log information and password updates are automatically consolidated across the domain.

Diagnostic Tools

BoKS Access Control for Servers provides a number of tools available directly from the command line for over viewing, analyzing and troubleshooting activity on protected hosts across the domain. Among them are:

- A program that takes a snapshot of the Master with version number, OS, patch levels, various BoKS Access Control for Servers configuration settings, and the most recent parts of the logs.
- Measuring the number of authentications per minute for a given Master or Replica and system-wide
- Debugging that can provide detailed output on a specified component or module
- The ability to produce utilization metrics from key daemons.

Update Tool

This tool makes it easy to push out patches, hotfixes and version upgrades to maintain BoKS Access Control for Servers at its best. It automatically installs or backs out a specified update on an entire Host Group or list of specified hosts. Or it can be run for information only to show, for example, which versions are installed on hosts across the network.

● System Architecture

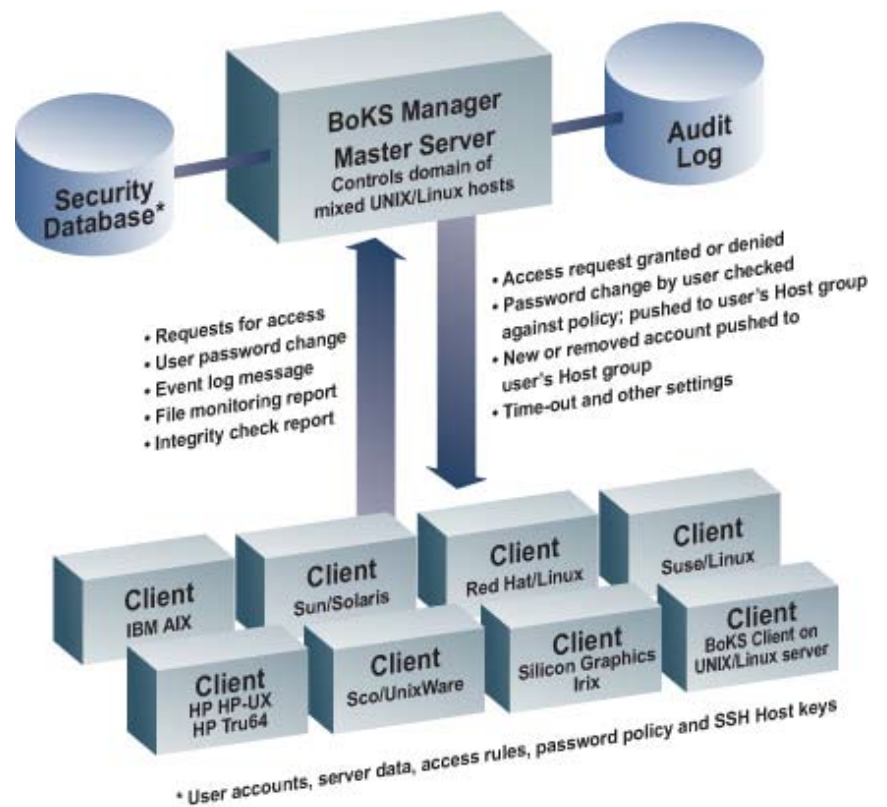
BoKS Access Control for Servers architecture is robust, flexible, secure and highly configurable. This section describes key aspects of its architecture. Topics include:

- Client/Server Architecture for a Domain
- System Programs Replaced by BoKS Access Control for Servers
- Access Control Mechanisms
- How BoKS Access Control for Servers Protects UNIX/Linux Hosts
- Auditing
- User Administration
- Administration Interfaces

Client/Server Architecture for a Domain

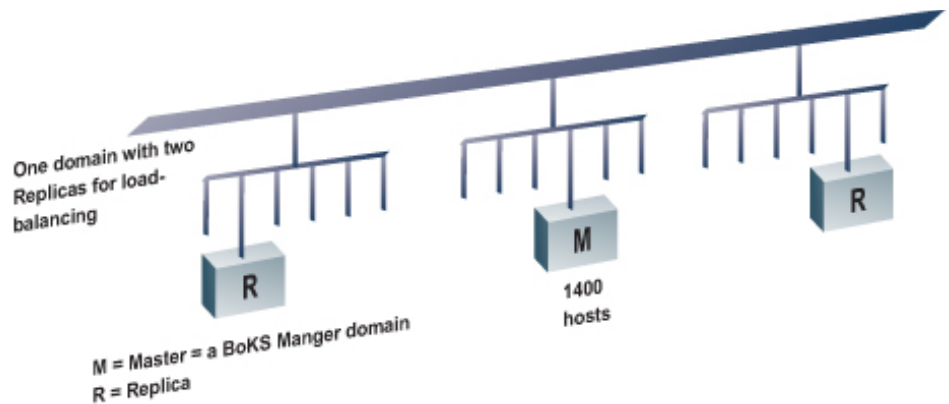
BoKS Manager is the server-based platform for the BoKS Access Control for Servers solution. BoKS Client for UNIX is the client software installed on each UNIX or Linux host to protect it.

In a network, you can have several installations of the BoKS Access Control for Servers solution. Each installation is called a **security domain** and is made up of one **BoKS Manager Master** server and any number of UNIX/Linux hosts, which are termed **Clients** or **BoKS Clients**. Optionally one or more **BoKS Replica** servers can be installed to back up the Master server.



Redundancy and Load Balancing

The Master server is the central point at which administrators manage the security domain. Each Replica server houses a complete, updated, read-only copy of the security database, thereby providing failover redundancy, scaling capability, and load balancing. Number and placement of Replica servers is entirely discretionary and dependent on size of domain, number of authentications per minute, etc. One simple setup is to place a Replica on each major subnet to handle access requests for that network, as illustrated below.



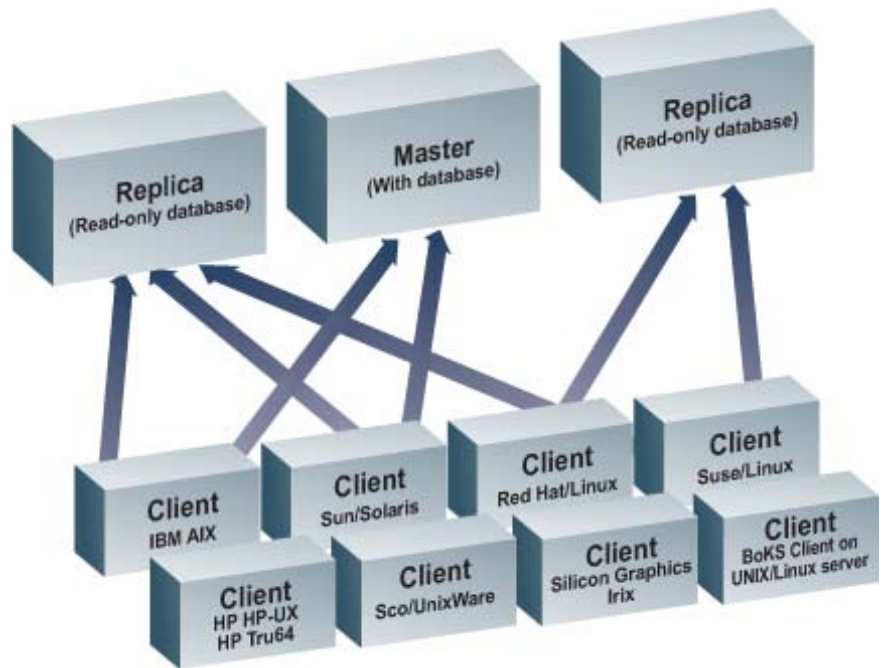
BoKS Access Control for Servers Security Domain

All updates to the security database are handled by the Master server. When an update occurs, the Master server updates its own database and then sends this update to the Replica servers' databases. The Master server also keeps the **/etc/passwd** and **/etc/group** files or TCB updated on machines in the security domain.

Log files can be replicated for backup redundancy on any Replica. To limit log traffic, log replication can be configured to include only the most important Replica servers.

Automatic Load balancing

Each Client can be configured with a list of Master and Replica servers to contact. Which of these servers actually responds to a given request for service is dependent on BoKS Manager's built-in load balancing. Each Master and Replica server operates a queue that handles incoming requests. The server monitors the number of requests in its queue and begins to slow the process of taking calls when this number reaches a given limit. When it reaches the maximum incoming request limit, it stops taking calls altogether. This is crucial because all BoKS Access Control for Servers servers time-stamp each request and have an internally set limit of 20 seconds for handling a request.



Request for access handled by the first available Master or Replica Server

Multiple server daemon processes can be configured on the Master and Replicas to increase capacity to handle client requests.

Failover

With the BoKS Access Control for Servers replica system, it is simple to convert a Replica to a Master, if necessary. The conversion program performs this task in less than one minute.

Automatic Client Registration

You can pre-register BoKS Clients in the BoKS database and set them to be automatically added to the BoKS domain whenever they are online and removed when they are offline. This feature can be useful for machines that are only used periodically or sporadically in your network, such as virtual machines only employed at peak processing times. Automatic client registration ensures that machines are instantly afforded the management and protection benefits of the BoKS domain when used, and automates user password updating.

Communication

Internal communication uses TCP/IP and is encrypted using the RC5 128-bit standard. Communication can be divided into three types: updating, replication, and authentication requests.

For authentication requests, there are two ways in which BoKS Access Control for Servers clients can contact the Master and/or Replica servers: by broadcast (default) or by addressing the servers directly. These are configurable, so that each Client can call those and only those Replicas that are appropriate for the given network structure (for example, considering subnets in distant buildings or countries).

The Master and Replica hosts must have static IP addresses, but BoKS Client for UNIX hosts can have either static or dynamic IP addresses, so may be deployed in DHCP environments.

Ports

BoKS Access Control for Servers allocates four ports for communication (registered at IANA). Each port has its own daemon to take calls. The ports are as follows:

- 6500 – Used by the master daemon. The master daemon updates the Master server's data base, as well as initiates the replication.
- 6501 – Used by servm daemon. The servm daemon has the task of updating the Replica server databases.
- 6502 – Dedicated for any requests. The daemon servc listens on this port to handle requests for authentication and authorization.
- 6503 – Used for updating /etc/passwd or TCB through the clntd daemon.
- 6505 – Used for remote administration via the graphical user interface.

These are the default ports for a domain and can be reconfigured for use of multiple domains or if these ports are already dedicated.

Encrypted communication

When two BoKS Access Control for Servers machines communicate, they use node keys as a shared secret for encryption. These node keys are assigned to each machine during setup and are registered on the Master. When the node key is assigned, it is md5 hashed (128-bit) and the hash used as the encryption key.

System Programs Replaced by BoKS Access Control for Servers

During the installation process, BoKS Manager and BoKS Client for UNIX do not modify the system kernel. Instead, they install BoKS-enhanced versions of access programs such as **login**. When you activate **BoKS Protection** on a server, these enhanced versions replace the originals, so that all authentication and authorization is redirected through BoKS. You can deactivate Host

Protection on a server at any time, in which case the original access programs are put back in place, and the system functions as previously configured without BoKS.

The solution includes tools to customize what services are activated depending on whether or not BoKS protection is active on a host, enabling you to tailor system settings to your security policy.

For PAM platforms, the architecture is different. PAM is left in control, but configured to call BoKS for authentication and authorization. Again, this configuration is done on activation of BoKS Protection and reverts back to the original configuration when you deactivate BoKS.

Access Methods

BoKS Access Control for Servers supports the following protected services:

- **login** - Supports login from ttys to a target host/Host Group. Authentication requires username and code (password or passcode). All login requests are registered, and log entries contain time, tty, target machine, username, and method of authentication.
- **telnetd** - Supports login from a source host/Host Group to a target host/Host Group. Authentication requires username and code. Can be configured to provide secure single-sign-on services for communication between servers using a proprietary protocol, within the BoKS Access Control for Servers domain. All requests are registered, and log entries contain time, source/target hostnames, username, and authentication method.
- **rlogind** - Supports remote login from a source host/Host Group to a target host/Host Group. Authentication requires username with target user code or no code at all. All requests are registered, and log entries contain time, source and target machine names, target username, and method of authentication.
- **rshd** - Supports rlogin from a source host/Host Group to target host/Host Group. Authentication requires target username with target user code. All requests are registered and log entries contain time, source and target machine names, target username, method of authentication and command given. **rsh** is strengthened under BoKS Access Control for Servers by requiring login and by overriding any .rhosts files and instead centrally managing rsh via BoKS Access Routes. This access method also includes remote copy (**rcp**).
- **rexecd** - Supports rexec from a source host/Host Group to target host/Host Group. Authentication requires target user code. All requests are registered, and log entries contain time, source and target machine name, target username, source username, method authentication and command given.
- **ftpd** - Supports ftp from a source host/Host Group to target host/Host Group. Authentication requires target username and target user code.

All calls are logged in the log database with time, from machine, target machine, target username, and method of authentication.

- **su** - Supports su from a tty to target user at host/Host Group. Authentication requires target username and target user code or source user code, provided the user is allowed to **su** to another user using the code for the source user as authentication. All calls are logged in the log database with time, from machine, target machine, target username, source username, and method of authentication.
- **suexec** - Supports running an allowed command with suexec on a target machine as another user, such as root, given source user code. All calls are logged in the log database with time, from machine, target machine, source user name, command, and method of authentication.
- **xdm** - Supports xlogin from a source host/Host Group to target host/Host Group. Authentication requires target username and target user code. All calls are logged in the log database with time, from machine, target machine, target username, and method of authentication.
- **sshd** - Supports ssh login from a source host/Host Group to target host/Host Group. All calls are logged in the log database with time, from and target machine, target user and method of authentication. Detailed, granular control is provided by requiring that user must be assigned both a general SSH access route for SSH authentication and one or more of the following SSH services:

SSH_X11	X11 tunneling
SSH_SH	Interactive shell
SSH_EXEC	Command execution
SSH_SFTP	SFTP subsystem
SSH_RFW	Remote TCP port forwarding
SSH_FWD	TCP port forwarding
SSH_SCP	Remote copy

SSH is strengthened under BoKS Access Control for Servers by requiring an Access Route, which allows service granularity as well as control of source and target hosts, times of day, etc.

Access Control Mechanisms

Authenticators

BoKS Access Control for Servers is configured by default for password authentication, using the password stored in the BoKS Manager database (not the password in the local system's passwd or shadow file).

Strong authentication is available for use whenever a password alone is not secure enough. BoKS Access Control for Servers can be configured to provide strong authentication with RSA SecurID® tokens, Secure Computing SafeWord® tokens, SSH Public Key, and SSH Hostbased and SSH Certificate authentication. The BoKS Manager Authenticator interface is flexibly de-

signed to allow smooth plug-in integration with new Authenticators for two-factor or PKI-based authentication as needed.

Authentication Method

In BoKS Manager, you can specify not only which authenticator is to be used, for example, SecurID token, but how, when and where it is to be used, for example, required for administrators for telnet access to certain hosts. Such a specification for how the authenticator is to be used is called an Authentication Method. Examples of Authentication Methods are mandatory or non-mandatory one-time passwords and mandatory or non-mandatory SSH Public Key.

When a method is mandatory for an Access Route, all users are required to authenticate with that method on that route. When a method is non-mandatory, it is required only for those users who are configured with the corresponding authenticator (for example, a token), while other users are allowed to log in with their BoKS Access Control for Servers passwords.

Access Route

Every access, to be allowed by BoKS Access Control for Servers, must fall under one or more rules, called Access Routes, that the user has been assigned. An Access Route specifies how, from where, and when a user may access a particular host or group of hosts. An Access Route includes:

- User or User Class
- Access Method (telnet, ftp, login, ssh, etc.)
- Source and destination computers ("from host", "to host")
- Day of week and time of day when access is to be granted

BoKS Access Control for Servers allows you to control access to UNIX environments by assigning Access Routes to users individually or by User Class.

A Restricted Access Route is an Access Route that denies access. A restricted Access Route takes precedence over all non-restrictive routes. It can be used to remove part of the access that a user inherits from membership in a User Class, that covers more access than the user really needs but that is convenient for administrative purposes.

Execute as Root

Authorization to execute as root can be granted to users separately for specified programs using the BoKS Access Method **suexec**. Suexec can be used to allow users to perform operations requiring root privileges without having to actually become root. All suexec commands are logged, and can optionally be keystroke logged for maximum traceability.

User Class

A User Class is a group of users with similar access needs, defined by the organization for ease in managing access rights. Individual users are normally, but not necessarily, assigned to one or several User Classes. Members of a User Class inherit all the Access Routes of the particular User Class. A user's total access is the sum of his/her User Class inherited routes plus any individually assigned routes, including any restrictive (denied) routes.

Host Group

A Host Group is a collection of UNIX/Linux host computers defined by the system administrator for ease in managing access rights and user accounts. Individual hosts are normally, but not necessarily, members of one or more Host Groups. If a user account is added to a Host Group, BoKS Access Control for Servers maintains the user account on all the individual hosts included in the group. Furthermore, Access Routes can be based on Host Groups rather than individual hosts, which makes it easy to define a structured scheme for access control in very large networks.

User access request

On the client side, users may access a BoKS Access Control for Servers-maintained host through any of the various access programs that BoKS Access Control for Servers supports.

Login request format varies depending on which access program is used. For example, a service such as rshd could grant access to a system without requiring a password, and su could accept the user's own password rather than the password of the target user. However, in most cases a username and the corresponding password or, if the Access Route requires strong authentication, the corresponding Authenticator, is required. When access is denied, the reason is logged, but the reason is by default not displayed to the user (unless you specifically configure it) and BoKS Access Control for Servers completes the whole process, for example, asking for username and password or passcode, so that an attempted intruder gains no information from the failure.

How BoKS Access Control for Servers Protects UNIX/Linux Hosts

User access authentication and authorization process

When a user attempts to log in at the BoKS Client for UNIX node, the node begins by locating an available authentication server, that is, a BoKS Master or Replica. The login request is then forwarded to the first server that responds, which compares the login request with the settings in the security

database. It first checks if the Access Route has any particular settings, for example, whether the Access Route requires SecurID or SafeWord authentication. Next, the Client requests the username (this is not applicable in a single sign-on connection) and sends it to the authentication server. At the same time, it queries the server to learn if anything special is required for this user to gain access, for example an RSA SecurID or SafeWord passcode. In the last step of the authentication, the Client sends the passcode or password to the server for determination whether the user is allowed to access the machine. After the authentication server has processed the information, the sequence ends with the Client sending a log entry to the Master. Regardless of whether the login request is granted or denied, the event is written to the BoKS Access Control for Servers log.

Node Keys for Encrypted Communication

To encrypt communication, BoKS Access Control for Servers uses a Node Key that is a unique password given to each host within the BoKS Access Control for Servers domain. The Node Key is also used to authenticate a BoKS Client when it communicates with the BoKS Master or Replicas. The Node Key is part of the unique session key used for encryption during the secure transmission between BoKS Client and Master or Replica.

Integrity checks

The BoKS Access Control for Servers integrity check reviews a UNIX/Linux system looking for configuration vulnerabilities. Automatic integrity checks are run by cron and manual checks by an administrator on demand. Checks generate reports in text file format that are sent to the Master for archival and/or further analysis.

Checks can be configured on a host basis to include (or not include) the following items:

- **rc files** - Checks if `/etc/rc` and the programs referenced in the rc files are writable. This check also includes `/etc/inittab` and `/sbin/init`, and files referenced from these files.
- **crontab files** - Checks the root crontab for writability. The commands used in the crontab file and any embedded file references are also checked for writability. Each command is checked to ensure use of absolute path names.
- **file permission check** - Scans all local file systems to find suspicious permissions, names, or ownerships. This is performed through a comparison against a list of known permissions and ownerships in the files `/etc/opt/boksm/bic/checks.conf`, `./permlist.conf`, and `./system.conf`. This check also includes search device nodes located outside `/devices` or `/dev`, and `setuid` files writable by no one but the owner. `Setuid` root files are always reported unless they are present in the list of known

permissions and ownerships.

- **mounted File system;** Device files - Checks permissions in the `/etc/fstab`. Writable and world-readable devices are reported.
- **NFS exported and mounted file systems** - Checks security problems related to NFS, such as unrestricted exports and mounting with `suid` enabled.
- **passwd file** - Checks the format of the `passwd` file(s). Potentially illegal lines are reported.
- **UNIX Mailbox Directory**- Checks the files in the mail directories for suspicious names, modes, permissions, or types. The check reports if a file is not named after its owner and if a file is readable by anyone other than the owner or a special mail group.
- **inetd config file** - Checks the `inetd.conf` and `/sbin/inetd` for vulnerabilities. This also includes programs called from `inetd.conf` as `root`.
- **TFTP configuration** - Checks that `tftp` is not configured in a way that any file on the system can be accessed via `tftp` from anywhere.

File monitoring

The file monitoring daemon surveys directories and files, looking for changes over time that would indicate intrusion or manipulation. It can be configured to check a file or directory for any of the following: `uid`, `gid`, permissions, `inode` number, modification time, creation time, and checksum. There are two different file monitoring features in BoKS Manager, one for the BoKS system itself and one that can be used for user files:

- **BoKS File Monitoring** is enabled by default and runs according to a preset configuration that includes all BoKS system sensitive files. It runs every second hour and reports any problems to the BoKS audit log.
- **Custom File Monitoring** runs on a customized set of directories and files, checking configured attributes and writing to either the BoKS audit log or a separate local file. The configuration file syntax is flexible, allowing administrators to define different types of actions on different directories or directory tree structures, and run interval. Wildcards allow ease of directory and file specification.

Auditing

BoKS Access Control for Servers centralizes the security logging function for the entire domain. Maintained on the Master, it can also be configured for backup on any Replica. It logs all activities that influence system security, such as changes to security parameters (collected in the System Log) and access attempts (collected in the Session Log). In addition, a local error log on the Master, Replicas and each Client host records technical problems such as daemon malfunction and inability to communicate with the Master, or, on the Master, inability to reach Replicas.

Event severity, preset at installation and modifiable, allows defining the highest priority events as alarm events. Alarm event messages can be sent to any program of the administrator's choosing. Following are some of the major log events:

Log Type	Event	Alarm
System	Any action carried out in Fox Server Control that affects the security database. This includes creating a user, changing security parameters, and registering a new host.	NO
System	Results of file monitoring	YES
Session	Logins and logouts, including network sessions	NO
Session	Unsuccessful login attempts, including network login attempts	NO
Session	Attempts to use non-interactive access programs	NO
Session	Attempts to use su	YES
Session	Password changes	NO

All logs are text-based and can be exported to other systems for analysis or surveillance. The GUI provides basic query functionality that allows quick extraction of messages by type, user, host, severity and free-text search.

User Administration

A user always belongs to one or several machines installed with BoKS Access Control for Servers. If systems already have users configured, BoKS Access Control for Servers can import them from any file in `/etc/passwd` format, NIS or LDAP. Imported users are added to either a single host or a predefined group of machines (Host Group). The use of Host Groups makes it easy to change the machines to which a user or group of users belongs. The administrator simply adds or deletes hosts in a Host Group.

BoKS Access Control for Servers can add and remove users, as well as update their account data, via LDAP synchronization. When specifying an LDAP provisioning path, user templates can be set to pre-define values for various UNIX and BoKS Access Control for Servers parameters such as primary and secondary group, User Class and home directory, for when any parameter does not exist in the LDAP data.

When a user is created, BoKS Access Control for Servers creates home directories and sets up profile files for each host belonging to a Host Group. BoKS Access Control for Servers adds, modifies, and deletes the user in a local `/etc/passwd` file, TCB, or in a NIS database.

For initial provisioning of Access Routes for users, BoKS Manager can run in **Learn Mode**. This bypasses Access Route checking and allows all requested access (providing that authentication and account requirements are met). Each access is logged with a special tag to provide Administrators with listings of actual user access services and paths, from which suitable Access Routes can be designed. Learn Mode simplifies and smooths startup of BoKS Access Control for Servers protection in the network.

Administration Interfaces

Graphical User Interface

The Graphical User Interface (GUI) is based on HTML code generated by TCL. This allows an organization to customize the interface. The GUI is equipped with default values that make it easy to begin managing the system. The http server uses SSL, which provides a secure connection between the browser and the Master.

For a remote connection, the administrator is required to have either a certificate or RSA SecurID token for authentication and an Access Route to the Master. For quick start up, password authentication to the GUI can be temporarily allowed, then disallowed after certificates or SecurID tokens have been distributed to administrators.

Access to the GUI is controlled by a special GUI Access Route. By default, this route grants access to the entire GUI. Using the Sub-Administrator menu, access for any individual can be limited to specifically configured menus, Host Groups, user accounts, etc, in order to delegate only the authority needed by that sub-administrator. This also allows delegating authority along organizational boundaries.

An Administration Wizard helps you configure the GUI for the first time, for quick startup of remote administration.

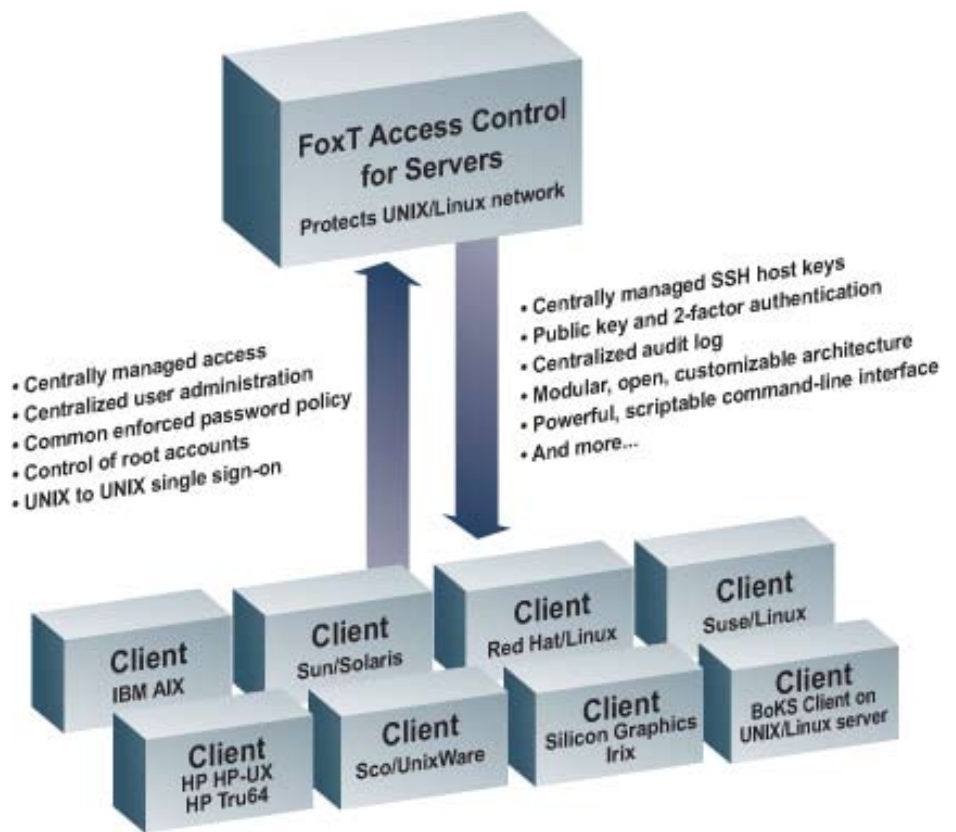
Command Line Interface

BoKS Access Control for Servers is based on a set of modular programs that allows you to perform tasks directly from the command line. The versatility of the CLI includes the whole range of scripting and configuring the security domain with tailor-made values. The CLI contains script templates that can

be used to perform tasks in the BoKS Access Control for Servers GUI after a user has been added, modified, or removed.

Access to the CLI is controlled by ordinary Access Routes. For example, an administrator can be granted an SSH Access Route from his or her workstation to the Master to provide a secure channel for administration. You can also use the pre-defined User Class called ADMIN, which includes pre-defined Access Routes for all services (ssh, rsh, login, etc.), from all hosts to all hosts. This class can be modified and tightened as appropriate, or administrators can be configured with Access Routes in other ways.

Besides administration, the command line modules are extremely useful for troubleshooting and debugging, and for customizing BoKS Access Control for Servers to local requirements.



BoKS Access Control for Servers Summary



FoxT
883 N. Shoreline Blvd.
Mountain View, California 94043
www.foxt.com
650.687.6300

Copyright © 2008 FoxT. All rights reserved.
The document is provided for informational purposes only and the contents herein are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior permission.

FoxT logo is a trademark of FoxT, Inc. Other product and company names herein may be registered trademarks and trademarks of their respective owners.