Server Suite

Unix and Linux User's Guide

Version: 2024.x

Publication Date: 7/26/2024

Server Suite Unix and Linux User's Guide

Version: 2024.x, Publication Date: 7/26/2024

© Delinea, 2024

Warranty Disclaimer

DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS, THE SOFTWARE AND SERVICES, AND OTHER MATERIAL PUBLISHED ON OR ACCESSIBLE THROUGH THIS SITE FOR ANY PURPOSE. ALL SUCH MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO SUCH MATERIAL, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

THE MATERIAL PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE MATERIAL DESCRIBED HEREIN AT ANY TIME.

Disclaimer of Liability

IN NO EVENT SHALL DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, PROFITS OR OTHER ECONOMIC ADVANTAGE) OR ANY DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR MATERIAL AVAILABLE FROM THIS SITE.

Table of Contents

User's Guide for Linux/Unix

The following topics are covered:

- [Introduction](#introduction)
- [Getting Started](#getting-started)
- [Troubleshooting](#troubleshooting)
- [Using the Command-Line Programs](#using-the-command-line-programs)

Introduction

This section provides an overview of what Server Suite software can do for Linux and UNIX computers, and how your administrator uses the Server Suite Agent to configure roles with specific rights to allow you to perform administrative tasks locally on your computer or remotely on a network server.

What is Server Suite

Server Suite provides a multi-tier software solution for IT administrators to centrally manage access rights and identity profiles for servers and workstations, mobile devices, and applications across a broad range of platforms. With Server Suite, administrators can accomplish the following:

- Manage local and remote access to computers with Linux, UNIX, Mac OS X, and Windows operating systems.
- Enforce security policies and control access to applications on mobile devices such as iPhone and Android smart phones and tablets.
- Enable single sign-on and role-based rights for on-site and cloud-based applications.
- Capture detailed information about user activity and the use of administrative privileges.

Using Server Suite, an Active Directory administrator creates zones to organize the enterprise's on-premise computers, mobile devices, and applications into groups. For each group, the administrator then defines rights, roles, and group policies to control access to the computers and applications in that zone. By using zones and role assignments, the administrator can establish fine-grained control over which users are authorized to perform certain administrative tasks and during exactly what time-frame, and when user activity should be audited.

With Server Suite, administrators can reduce the risk of unauthorized access to your organization's critical resources, ensure accountability and regulatory compliance for users granted access to privileged accounts or sensitive information, and simplify the management of shared accounts and role-based access rights. Additionally, Server Suite allows administrators to use the same account information for users across all platforms using a single account name and Active Directory password.

Types of Access Rights

In addition to the predefined UNIX Login role that grants basic access to Server Suite-managed computers during deployment, there are other common, predefined access rights and role definitions that may be available to you.These other predefined rights and roles definitions provide specialized access rights for specific scenarios that are common in Linux and UNIX environments.

Rype of Right	What a role with this type of right allows you to do
Command rights	Run the specified commands, which perform privileged operations, using a dzdo command.
PAM application rights	Run a specific PAM application that has elevated privileges.
Secure shell session-based rights	Access specific secure shell services for remote connections.

Every role includes one or more rights. Depending on the roles you have been assigned, you might have one or more of these access rights available.

Auditing Role-Based Activity

Your administrator may configure auditing to either record certain commands that you execute, or to record all of the terminal activity on your computer.

If the computer you are using is configured to audit session activity, you will only be notified that your actions are being audited if the administrator has enabled an auditing notification.

How Access to Computers Might Change

To manage access to UNIX and Linux servers and workstations, an administrator installs the Server Suite Agent on each computer and identifies the zone the computer should use. If an administrator has installed the agent on your computer and added your computer to a zone, your computer is a Server Suite-managed computer. When you log in to your Server Suite-managed computer, the agent checks whether you have been assigned a role for logging in which allows you to log in locally with a password, log in remotely without a password using single sign-on, and run commands in a standard shell or a restricted shell. As long as you have a role assignment that allows you one of those basic login rights, logging in proceeds normally. If you have not been assigned a role that allows you to log in, you will be denied access to the computer.

In most cases, an Active Directory administrator or another delegated administrator will also define rights and roles that enable you to use an account other than your own that has elevated privileges. For example, the administrator might create a role that allows you to manage an Oracle service account using administrative privileges and another role that enables you to use the file transfer protocol (ftp) to connect to another machine.

The administrator is responsible for defining the specific rights that are available in different roles and for assigning those roles to the appropriate Active Directory users and groups. The administrator can also assign selected roles to local UNIX and Linux users and groups.

What Gets Installed on a Managed Computer

When the Server Suite Agent is installed, your computer is updated with the following directories and files:

This Directory	Contains
/etc/centrifydc	The agent configuration file and the Kerberos configuration file.

This Directory	Contains
/usr/share/centrifydc	Kerberos-related files and service library files used by the Centrify Agent to enable group policy and authentication and authorization services.
/usr/sbin/usr/bin	Command line programs to perform Active Directory tasks, such as joining a domain and changing a user password.
/var/centrify	Directories for temporary and common files that can be used by the agent.
/var/centrifydc	The IP address of the DNS server, details about the software you have installed, the Active Directory domain the computer is joined to, the Active Directory site the computer is part of, and other details.
/var/log	Error messages, warnings, and informational messages, along with other kernel and program messages.

Depending on the components you select during installation, the Server Suite Agent might include additional files and directories. For example, if you install auditing services, your computer is updated with the additional files and directories required for auditing.

The Server Suite Agent also installs manual (man) pages to assist you in finding information on command line programs. For more information about using man pages, see "Displaying Usage Information and Man Pages" on page 9.

Getting started

This chapter describes how to use Server Suite to access applications and run commands with privileges on a UNIX or Linux computer that has the Server Suite Agent installed.

- Verify Login
- Checking Your Rights and Role Assignments
- Working with Command Rights
- Using PAM Application Rights
- Using Secure Shell Session Rights
- Role-based Auditing of Session Activity

Working with Command Rights

Command rights allow you to use commands to perform specific operations. The most basic rights such as the right to log in are defined when your administrator defines roles. Other, more granular command rights control access to individual command-line programs.

Using Command Rights in a Standard Shell

Command rights are assigned to you so that you can perform privileged operations that are not available to you by default.

On most UNIX and Linux computers, commands that require elevated permissions can be run by invoking the sudo command. The Server Suite Agent provides similar functionality, but the commands are instead invoked using the dzdo command, then typing the command to execute, including any command-line options that you are allowed to use.

For example, assume your administrator has defined a command right for adjoin that enables you to execute the command as the root user. If this right is added to a role that has been assigned to you, you can execute the command by typing the following:

```
dzdo adjoin
```

Using Command Rights in a Restricted Shell Environment

Server Suite provides a customized Bourne shell, dzsh, to serve as a restricted shell environment that is used to limit what commands you can execute for certain roles. For most operations, working in the dzsh shell is similar to working in an unrestricted shell except that the command set is limited to the command rights added by the administrator.

After your administrator has defined command rights, added them to role definitions, and assigned the roles to you, you can execute those commands in a restricted shell environment by typing the command, including any command-line options you are allowed to use. When you are finished running the command, you can switch back to your standard shell if you have the appropriate login right on that computer.

For example, assume that on your own computer, you can run the adinfo command in the standard shell, but you need to execute the command on a computer that is not yours. Your administrator has assigned you a role, AdminADinfo that grants you a UNIX login right and a right that requires you to run the adinfo command in a restricted shell on the computer you need to access. You must switch to this role to run the command on the specified computer. To do this, you log in to the computer you want to access and select the role your administrator has assigned to you. If you are a member of the zone Headquarters, you would type the following:

```
$ dzsh
$ role AdminADinfo/Headquarters
$ adinfo
```

Running Unauthorized Commands

If your administrator has assigned you to a role that requires a restricted shell environment, the dzsh shell allows you to run only the subset of commands to which you have rights. If you attempt to run a command you are not authorized to use in your current role, the shell displays a warning.

Setting or Changing your Active Role

If you are assigned only to one or more restricted shell environment roles, you are only allowed to run commands within the dzsh shell. Within the restricted shell, you can only be in one active role at a time to prevent ambiguity about the commands you can run or what account should be used to execute those commands.

For example, if you are assigned the lab_staff restricted shell environment role that specifies that the tar command should run as root, and also the temps restricted shell environment role that specifies that the tar command should be run as the account tmp_admin, you need to specify which role you are using to run the tar command under the proper account.

You can see what roles are assigned to you, as well as switch between roles, using the role command. For example, to view the list of roles to choose from, you would type:

```
$ role -ls
```

To choose the lab_staff role, you would type:

```
$ role lab_staff
```

Checking Your Rights and Role Assignments

Your role assignments control where you can log in, the type of account you use to log in, the specific access rights you have on local or network computers, the types of commands you can execute, and whether you must log in using a restricted shell. As discussed in Types of access rights, there are three categories of access rights for UNIX and Linux computers:

- Command rights
- PAM application rights
- Secure shell session-based rights

Depending on the details of how roles are defined in your organization and the specific roles you have been assigned, you might have some or all of the access rights described in the following sections.

You can use the dzinfo command to look up detailed information about your rights and role assignments, any restrictions on when they are available, and what the roles allow you to do. To learn more about the dzinfo command, see Check your rights and roles using dzinfo.

> You can view information about your own access rights and role assignments only.

Role-based Auditing of Session Activity

Your administrator may install the Server Suite Agent with or without auditing features. Depending on whether auditing features are activated on your computer and whether your role requires auditing or not, your session activity might be captured and stored in a database. You can check whether session-level or desktop auditing is requested or required for the roles you are assigned by running the dzinfo command. You are notified that your session activity might be audited only if the administrator has enabled notification. If auditing is required for your role, but the auditing service is not available on computer you attempt to use, you will be denied access to that computer until auditing is available.

If your administrator has configured the Server Suite Agent to audit your session when you log in, everything you do on your terminal is captured, including all of your keystrokes and anything displayed on your screen. If your administrator has configured auditing on a per-command basis, auditing only begins when you use a privileged dzdo command, and ends when you are finished running those privileged commands.

If your administrator has configured desktop auditing, everything you do in the Linux graphical user interface is captured. Note that for web browser activity, desktop auditing captures the web page title but not the contents or activity within a web page.

Using Secure Shell Session Rights

If your administrator has assigned you the sshd or ssh right, login-all right, or a custom PAM access right, you can use secure shell rights to perform specific operations on remote computers. The following are a list of predefined secure shell session-based rights that might be assigned to you:

- dzssh-all grants access to all available secure shell services.
- dzssh-direct-tcpip allows local and dynamic port forwarding (ssl-L, ssh -D).
- dzssh-exec allows command execution.
- dzssh-scp allows secure copy (scp) operations.
- dzsh-shell allows secure terminal (tty/pty) connections.
- dzssh-Subsystem allows external subsystems, with the exception of the sftp subsystem, which has its own right.
- dzssh-tcpip-forward allows remote port forwarding (ssh -R).
- dzssh-tunnel allows tunnel device forwarding.
- dzssh-x11-forwarding allows X11 forwarding.
- dzssh-sftp allows SSH File Transfer Protocol.

    > **Note:** Starting in the Server Suite 2023.1 release, the scp command's default protocol is now the sftp protocol. When scp uses the sftp protocol it is required to assign `dzssh-sftp` to the user. When the scp protocol specifies the `-O` option, it is required to assign `dzssh-scp` to the user.

Using PAM Application Rights

Most of the applications you run on Linux and UNIX computers are configured to use a pluggable authentication module (PAM) to control access. Secure shell (ssh), login, and file transfer (ftp) services are all examples of PAM-enabled applications.

If you have a role assignment with access to PAM-enabled application rights, you can run one or more specific applications using the administrative privileges defined for your role. The administrator defines the specific PAM application rights that you have in each role you are assigned. If you have a role assignment with application access rights, the administrator specifies the arguments you can use when running the application and the account used to run the application.

Verifying You Can Log in

If an administrator has installed the Server Suite Agent on a UNIX or Linux computer you use, the next step is to verify that you can log in successfully. The Server Suite Agent does not change how you log in to your computer. However, you must be assigned at least one role that allows you to log in.

When you are prompted for a user name and password, type your Active Directory or UNIX user name and your Active Directory password. If you provide valid credentials and have been assigned a role with permission to log in, you should be able to log in to your computer with a standard UNIX shell. If this is a computer you used earlier, before it became a Server Suite-managed computer, there should be no noticeable changes to your working environment.

As a part of the deployment of Server Suite software, your computer may or may not have been joined to a zone. To verify that the Server Suite Agent is installed, that you are connected to an Active Directory Domain, and that you

are connected to a zone, run the adinfo command. For example, if you are a user named billy in a zone named KHeadquarters, your output may look similar to the following:

```
[billy@kh-rh Desktop]\$ adinfo
Local host name: kh-rh
Joined to domain: demo.acme.com
Joined as: kh-rh.demo.acme.com
Pre-win2K name: kh-rh
Current DC: deploy.acme.com
Preferred site: Default-First-Site-Name
Zone: demo.acme.com/Program Data/Acme/Zones/KHeadquarters
CentrifyDC mode: connected
Licensed Features: Enabled
```

To learn more about commonly used commands that may be available to you, see Commands available for users.

If the Server Suite Agent is installed but not connected to a zone, or if the agent is not installed on your local computer, you should contact your administrator.

If the zone information for the agent is configured, but the agent status is Disconnected, restart the agent.

To restart the agent type the following:

```
\$ adclient -x
\$ adclient
```

If the agent status is still Disconnected, contact your system administrator.

Multi-Factor Authentication

Your organization may require multi-factor authentication in order for you to log in to your computer, or to execute commands using elevated privileges (dzdo) in a normal or restricted shell (dzsh) environment.

If multi-factor authentication is required as part of the login process, you will have to provide a password as well as a second form of authentication to log in to your computer. If multi-factor authentication is required as part of a re-authentication process, such as when you use command rights with elevated privileges or in a restricted shell, you must provide a password and either one or two other forms of authentication other than a password.

Using the Command-Line Programs

This section provides an overview of the available command-line programs that you can run on Server Suite-managed computers. If you have administrative rights on one or more Server Suite-managed computers, you have access to additional command line programs not described here.

Performing Basic Account-Related Tasks

Server Suite command-line programs are installed by default with the Server Suite Agent. The commands are typically installed in one of the following directories: /usr/sbin, /usr/bin, or /usr/share/centrifydc/bin.

Command-line programs allow you to perform basic Active Directory or UNIX administrative tasks directly from a UNIX shell or using a shell script. These commands use the underlying adclient service library to enable you to perform common tasks, such as changing your Active Directory password or setting your effective group membership. You can also use command-line programs to view information, such as the connection status and current zone for a managed computer or details about your effective rights and roles on a local host.

You should use the UNIX command-line programs interactively or in shell scripts when you must take action directly on a UNIX computer, or when taking action on the UNIX computer is most convenient. For example, if you typically log in to a UNIX terminal on a daily basis, you might want to change your Active Directory password by running a command in a login shell on that UNIX computer.

Commands Available for Users

Many of the Server Suite command-line programs require root privileges because they enable you to perform administrative tasks or operations that must be kept secure. In some cases, commands support different options or produce different results if run using an administrative account than when run using a standard user account.

The following table displays a brief description of the commands you can run when you are logged on as a standard user without elevated privileges.

Command	Description
adcheck	Check the operating system, network, and Active Directory connections to verify that a computer is ready to join an Active Directory domain. The syntax for the adcheck program is: `adcheck domain_name [options]` The domain_name should be a fully-qualified domain name.
adfinddomain	Display the domain controller associated with the Active Directory domain you specify. The syntax for the adfinddomain program is: `adfinddomain [options] domain_name`
adgpupdate	Retrieve group policies from the Active Directory domain controller and apply the policy settings to the local computer and current user immediately. The syntax for the adgpupdate program is: `adgpupdate [options]`
adid	Display the real and effective UIDs and GIDs for the current user or a specified user. The syntax for the adid program is: `adid [option] [username|uid]`
adinfo	Display detailed Active Directory, network, and diagnostic information for a local computer. Options control the type of information and level of detail displayed. The syntax for the adinfo program is: `adinfo [options] [--user username[@domain]] [--password password]`
adlicense	Display the current status of agent features on the local computer. Agent features can be licensed or express if unlicensed.
adpasswd	Change your Active Directory password. After you change your password, you must use the new password for all activities that are authenticated through Active Directory, including logging on to the UNIX shell, logging on to Windows computers, and accessing applications on both UNIX and Windows computers.

Command	Description
adquery	Query Active Directory for information about users and groups. This command is provided for backward compatibility. In most cases, you should use ADEdit (adedit) commands or scripts to perform administrative tasks in Active Directory from Linux or UNIX computers. The syntax for the adquery program is as follows: `adquery user|group [options] [username|groupname]`
adsetgroups	View or change the list of groups of which you are a member. The syntax for the adsetgroups program is: `adsetgroups [options] group`
adsmb	Perform file operations, such as get a file, write a file, or display the contents of a directory using the ## smb stack. The syntax for the adsmb program is: `adsmb file_operation -s share [options]` The valid file_operations are `get`, `getnew`, `put`, `putnew`, `dir`, `delete`, `mkdir`, and `rmdir`.
dzdo	Execute a privileged command as root or another specified user. The syntax for using the dzdo program is: `dzdo [options]`
dzinfo	Display detailed information about the configuration of rights and roles for one or more specified users on the local computer. If you do not specify a user, the command returns information for the currently logged on user. The syntax for the dzinfo command is: `dzinfo [options]`
dzsh	Run commands in a restricted environment shell. This shell is a customized Bourne shell that provides environment variables, job control, command history, and access to specific commands defined by roles.

For information about the additional commands available if you have root or root-equivalent privileges on a computer, see the _Administrator's Guide for Linux and UNIX_ or the _Server Suite Command Reference Guide_.

Displaying Usage Information and Man Pages

To display a summary of usage information for any command-line program, type the command and the `--help` or `-h` option. For example, to see usage information for the adleave command, type:

```
adleave --help
```

The usage information includes a list of options and arguments, and a brief description of each option. For example, if you specify `adleave -h` on the command line, the command displays the command-line syntax and a list of the valid options you can use when you execute adinfo commands, similar to the following:

```
usage: adleave [options]
options:
  -u, --user user[@domain] user name, default is administrator
  -p, --password pw        user password, prompts if absent
  -s, --server ds          domain server for leave operations
  -Z, --zoneserver ds      domain server for zone operations
                           useful if zone is in another domain
  -C, --noconf             do not restore PAM or NSS config
  -G, --nogp               do not restore Group Policy
  -f, --force              force local leave, no network activity
```

```
 -v, --version          print version information
 -V, --verbose          print debug information for each operation
 -r, --remove           remove computer account from Active Directory
 -R, --restore          restore system configuration files without leaving
 -t, --reset            using the machine credentials, reset computer to
                        pre-created/unjoined state
 -h, --help             print this help information and exit
```

For more complete information about any command, you can review the information in the command's manual (man) page. For example, to see the manual page for the adleave command, type:

```
man adleave
```

Troubleshooting

This section describes how to resolve problems you might encounter while attempting to log in.

Solving Login Problems

There are several reasons why an attempt to log in can fail. If you are denied access to a computer:

- Verify that the computer you are trying to log in to has access to an Active Directory domain controller. If an Active Directory domain controller is not available or the local computer is not a memberof an Active Directory domain, you might be prevented from logging in because the agent cannot verify that you have authority to access the computer.

- Verify that you have a complete UNIX identity profile.

- Verify that you have been issued at least one role with a right that allows you to log in using a standard shell or a restricted shell.

  If you have access only to a restricted shell, you can only execute explicitly defined commands.

  If you have a UNIX profile, but cannot log in to your terminal, you may have been assigned the `listed` or `local listed` role. These roles allow your profile to be visible in a zone, but do not grant any access rights.

  After the agent has been installed, you must have a role assigned to your account that gives you log in privileges. If an attempt to log in fails, contact your Active Directoryadministrator or help desk to determine the roles you have been assigned, the type ofaccess your roles grant, and any limitations associated with your role assignment. Forexample, roles can have time constraints with specific periods of availability. If youattempt to log in, but the role is not available at the time you attempt to log in, you will be denied access.

Check your Rights and Roles using dzinfo

You can use the dzinfo command to view detailed information about your rights, roles, and role assignments. The dzinfo command allows you to view and capture the output from the command in a single window.

For example, if you are a user named billy in a zone called KHeadquarters, you would type:

```
dzinfo billy
```

The output would look similar to the following:

```
User: billy

Forced into restricted environment: No

Role Name        Avail  Restricted Env
```

```
--------------   -----   --------------
AdminRole        Yes     Admin
/KHeadquarters           /KHeadquarters
Windows          Yes     Windows
Login/KHeadquar          Login/KHeadqua
ters                               rters
ControlPanelAdm  Yes     ControlPanelAd
in/KHeadquarter          min/KHeadquart
s                                  ers
UNIX             Yes     None
Login/KHeadquar
ters
Windows          Yes     Windows
Login/KHeadquar          Login/KHeadqua
ters                               rters
UNIX             Yes     None
Login/KHeadquarters

Effective rights:
Password login
Non password login
Allow normal shell
Audit level:
AuditIfPossible
Always permit login:
true
PAM Application  Avail Source Roles
--------------   -----  -------------------
graphical        Yes    AdminRole/KHea
desktop                  dquarters
ftp              Yes    AdminRole/KHea
dquarters
telnet           Yes    AdminAdminRole/KHea
dquarters
sshd             Yes    AdminRole/KHea
dquarters
ssh              Yes    AdminRole/KHea
dquarters
```

```
*               Yes   UNIX
Login/KHeadquarters
SSH Rights      Avail Source Roles
--------------  ----- --------------------
dzssh-sftp      Yes   AdminRole/KHea
dquarters
dzssh-scp       Yes   AdminRole/KHea
dquarters
dzssh-exec      Yes   AdminRole/KHea
dquarters
dzssh-shell     Yes   AdminRole/KHea
dquarters
dzssh-*         Yes   AdminRole/KHea
dquarters


Privileged commands:
Name            Avail Command   Source Roles
--------------  ----- --------- --------------------
dz_info/KHeadqu Yes dzinfo      AdminRole/KHea
arters                             dquarters
emergency_acess Yes su - root AdminRole/KHea
/KHeadquarters                    dquarters
emergency_acess Yes su - root UNIX
/KHeadquarters             Login/KHeadquarters
emergency_acess Yes su - root Windows
/KHeadquarters             Login/KHeadquarters


Commands in restricted environment:
Name            Avail Command   Run As
--------------  ----- --------- ----------
emergency_acess Yes   su - root self
/KHeadquarters


Commands in restricted environment:
ControlPanelAdmin/KHeadquarters
Name            Avail Command   Run As
--------------  ----- -------- ----------
(no commands have been configured for
```

```
ControlPanelAdmin/KHeadquarters)


Commands in restricted environment:
AdminRole/KHeadquarters
Name            Avail Command   Run As
--------------- ----- --------- ----------
dz_info/KHeadqu Yes   dzinfo    self
arters
emergency_acess Yes   su - root self
/KHeadquarters


Commands in restricted environment:
Windows Login/KHeadquarters
Name            Avail Command    Run As
--------------- ----- ---------- ----------
emergency_acess Yes   su - root  self
/KHeadquarters
```