EVIDEN

Identity and Access Management

DirX Directory

Supervisor

Version 9.1, Edition June 2025

Table of Contents

Preface

This manual is reference for the DirX Directory (DirX). It consists of the following sections:

- Chapter 1 provides information about the supervisor.

DirX Directory Documentation Set

DirX Directory provides a powerful set of documentation that helps you configure your directory server and its applications.

The DirX Directory document set consists of the following manuals:

- *DirX Directory Introduction*. Use this book to obtain a description of the concepts of DirX Directory.
- *DirX Directory Administration Guide*. Use this book to understand the basic DirX Directory administration tasks and how to perform them with the DirX Directory administration tools.
- *DirX Directory Administration Reference*. Use this book to obtain reference information about DirX Directory administration tools and their command syntax, configuration files, environment variables and file locations of the DirX Directory installation.
- *DirX Directory Syntaxes and Attributes*. Use this book to obtain reference information about DirX Directory syntaxes and attributes.
- *DirX Directory LDAP Extended Operations*. Use this book to obtain reference information about DirX Directory LDAP Extended Operations.
- *DirX Directory External Authentication*. Use this book to obtain reference information about external authentication.
- *DirX Directory Supervisor*. Use this book to obtain reference information about the DirX Directory supervisor.
- *DirX Directory Plugins for Nagios*. Use this book to obtain reference information about DirX Directory plugins for Nagios.
- *DirX Directory Disc Dimensioning Guide*. Use this book to understand how to calculate and organize necessary disc space for initial database configuration and enhancing existing configurations.
- *DirX Directory Guide for CSP Administrators*. Use this book to obtain information about installing, configuring and managing DirX Directory in the context of a Certificate Provisioning Service operating in accordance with regulations like the German “Signaturgesetz”.
- *DirX Directory Release Notes*. Use this book to install DirX Directory and to understand the features and limitations of the current release.

Notation Conventions

Boldface type
In command syntax, bold words and characters represent commands or keywords that must be entered exactly as shown.

In examples, bold words and characters represent user input.

Italic type
In command syntax, italic words and characters represent placeholders for information that you must supply.

[ ]
In command syntax, square braces enclose optional items.

{ }
In command syntax, braces enclose a list from which you must choose one item.

In Tcl syntax, you must actually type in the braces, which will appear in boldface type.

|
In command syntax, the vertical bar separates items in a list of choices.

...
In command syntax, ellipses indicate that the previous item can be repeated.

install_path
The exact name of the root of the directory where DirX Identity programs and files are installed. The default installation directory is *userID_home_directory**/DirX Identity* on UNIX systems and **C:\Program Files\DirX\Identity** on Windows systems. During installation the installation directory can be specified. In this manual, the installation-specific portion of pathnames is represented by the notation *install_path*.

1. DirX Directory Supervisor Scripts

The DirX Directory Supervisor consists of the **dirxsupervisor** command and a suite of Tcl- and Perl-based scripts that allow DirX Directory administrators to maintain high availability of directory data in DirX Directory floating master/shadow replication configurations.

The Supervisor scripts monitor the responsiveness of DirX Directory service floating-master instances (DSA and LDAP server processes) by issuing LDAP operations directed to the DSA and can recover from responsiveness problems using the DirX Directory client **dirxadm**.

The DirX Directory Supervisor include:

- The **dirxsupervisor** command that starts the DirX Directory Supervisor core script (**dirxsupervisor.tcl**).
- The DirX Directory Supervisor core script (**dirxsupervisor.tcl**), which is the main script used to monitor the DSAs and recover from responsiveness problems.
- The DirX Directory Supervisor setup script (**setup_common_data.tcl**), which is the configuration script that DirX Directory administrators can use to customize Supervisor script operation.
- The DirX Directory Supervisor common procedures script (**DxD-CommonProcs.tcl**), which contains common procedures used by the other DirX Directory Supervisor scripts.
- The DirX Directory Supervisor shadow operational bindings script (**SOBcmds.tcl**), which provides streamlined **dirxadm** command calls for shadow operational bindings.
- The DirX Directory Supervisor utility script (**cmdargs.tcl**), which passes parameters to an email client on a Windows platform.
- The DirX Directory Supervisor heartbeat script (**SVheartbeat.pl**), which performs the periodic checks that monitor a supplier or a consumer DSA in a floating master configuration.
- The DirX Directory Supervisor password file (**adm_pwd**).

The DirX Directory Supervisor core and setup scripts are intended for direct use by DirX Directory administrators and are highly customizable. The remaining scripts are called internally by the DirX Directory Supervisor core script and should not be customized.

1.1. General Information

This section provides general information about the Supervisor scripts, followed by reference pages for the **dirxsupervisor** command and **setup_common_data.tcl**.

1.1.1. Prerequisites and Limitations

The DirX Directory Supervisor scripts have the following pre-requisites and limitations:

- The following software packages to be installed on each Supervisor host machine:
- The Perl language/interpreter distribution, version 5.16.3 or newer.

- The perl-ldap distribution, which is a collection of Perl modules that provides an object-oriented interface to an LDAP server.

See the **ReadMe.txt** file in the Monitoring installation folder (*install_path**/monitoring*) for instructions on how to set up Perl on the supported DirX Directory platforms.

- If email notification is to be used, the freeware email Windows client binary **bmail.exe** must be installed on a Supervisor host machine running the Windows platform.
- The unit of replication must be the entire DIT (this is a requirement of a floating-master scenario).
- The scripts are intended only for monitoring floating-master configurations. They cannot be used to monitor a stand-alone DSA.
- The scripts currently do not provide a mechanism for automating state log collection, cataloging backup and analysis. It is the responsibility of the DirX Directory administrator to review and manage the generated state logs.

1.1.2. Installation Location

DirX Directory provides the DirX Directory Supervisor scripts in the location *install_path***/monitoring/supervisor**.

1.1.3. Script Operation

Each Supervisor script instance monitors the connectivity between a pair of DirX Directory DSAs - the supplier DSA and one consumer DSA.

A Supervisor script instance performs supplier-mode or consumer-mode monitoring and recovery operations depending upon the replication role of its local DSA. Supplier or consumer operating mode is determined on script startup and is periodically checked and automatically adjusted if the local DSA role changes as the result of a **dirxadm sob switch** operation.

The Supervisor scripts monitor shadowing responsiveness by periodically directing asynchronous LDAP operations (called heartbeat operations) to the local DSA and one remote DSA. The scripts require a specified bind DN and a test entry to perform these operations; specify these parameters in the **setup_common_data.tcl** script.

In supplier mode, the heartbeat operation is an LDAP bind as a Supervisor user entry (**SVuser** in **setup_common_data.tcl**) to the local DSA that adds a timestamp to the **description** attribute of a test entry (**testentry** in **setup_common_data.tcl**) or the Supervisor user entry, if no test entry is specified, and a subsequent read/compare of the test entry on the remote consumer DSA.

In consumer mode, the heartbeat operation is an LDAP bind as **SVuser** to the local (replicated) test entry's description attribute (or the **SVuser** entry, if **testentry** is not specified) and a subsequent read operation of the test entry on the supplier. See **setup_common_data.tcl** for a description of **SVuser** and **testentry** parameters and their requirements.

The Supervisor scripts monitor network responsiveness by periodically sending **ping** commands to a network router in the configuration or to the remote DSA, if no router is present (**routerIP** in the **setup_common_data.tcl**).

The Supervisor scripts attempt to recover from connectivity and responsiveness problems detected by their monitoring processes in two ways:

- By attempting to restart the DirX Directory service a configurable number of times (see the **retryCnt** parameter in the **setup_common_data.tcl** script)
- By performing an emergency switch to transfer mastership of the DIT to the consumer DSA, if repeated attempts to re-start the service fail.

The following table provides a quick reference of the types of responsiveness problems detected by the Supervisor scripts and the response depending on the operating mode (supplier or consumer).

Incident Detected	**Where Detected**		**Supervisor Response**	
	Supplier	**Consumer**	**Supplier**	**Consumer**
DirX Directory Service stopped	X		Restart service	Log problem
		X	Log replication problem	Restart service
DirX Directory Service restart error	X		Perform emergency switch to one of the consumers	Change role to supplier
		X	Log connection problem	Log restart error
LAN outage	X		Log LAN outage	Perform emergency switch to the local consumer
LAN and router outage	X		Log LAN outage	Log LAN outage
Heartbeat problem	X		Restart service	Log heartbeat problem
		X	Log heartbeat problem	Restart service
SOB disabled	X		Log SOB problem	N/A
		X	Log SOB problem	Log SOB problem
No incident	X	X	Log result of every heartbeat operation	Log result of every heartbeat operation

1.1.4. State Logging

Supervisor scripts generate state logs about the results of each monitoring and recovery operation. Supervisor script state logging is directed to standard out unless you (the DirX Directory administrator) explicitly redirect it to a file. There is currently no built-in mechanism for managing Supervisor state log output. DirX Directory administrators are responsible for keeping track of the state logging process and saving or backing up state log messages for analysis of recurring or long-term problems.

1.1.4.1. State Log Format

State logs are in the format:

timestamp: *msgType* {[*OpType* (*host*) *comment*] | [*comment*]}

where:

timestamp
Specifies the time at which the test operation was performed, in the (default) format *dd.mon.yyyy_hh:mm:ss*:. For example: **13.Dec.2013_16:49:18:**.

msgType
Specifies the Supervisor operation result and is one of the following values:

OK The operation has completed successfully.
POK *n* The operation has failed, and the configured number of follow-up operation retries will be performed, where *n* specifies the current retry count. For example: **POK 1**, **POK 2**, **POK 3**.
NOK The configured number of operation retries have all failed, and the appropriate follow-up recovery operation will be automatically performed, if one is available for the problem. If the problem requires manual follow-up action by the DirX Directory administrator, *comment* contains the text **administrative attention/intervention recommended**.
MSG Explanatory text about the operation.

OpType
Specifies the Supervisor operation that was performed. For example: **(getSUK) Local-AE-Show-1** where **getSUK** means get supplierKnowledge (either the local or the remote one) while **Local-AE-Show-1** means viewing the AE-Title attribute value of the local DSA instance.

host
Specifies the name of the DirX Directory service host on which the operation was performed. For example: **(TMP1-W2K8-R3)**.

comment
Provides an explanation of the operation result. For example, **DirX Directory -Start and LDAP connectivity passed**.

1.1.4.2. State Log Example

The following example shows the state log messages generated when the Supervisor

running on a supplier detects that the DirX Directory service has stopped.

The initial state log shows the Supervisor establishing its operation mode:

```
13.Dec.2013_16:35:20: MSG 1.(rolesCHeckNAME) InstanceRole detected:
Master (on SupplierDB)
```

The following state log indicates that a heartbeat operation has failed:

```
13.Dec.2013_16:37:11: POK 1.Heartbeat - general bind/modify problem
identified to supplier=tmp1-w2k8-r1 (1)
```

The next group of state logs shows that the follow-up operation **(getSUK) Local-AE-Show-1** is repeated three times, failing all three tries:

```
13.Dec.2013_16:37:36: POK 1.(getSUK) Local-AE-Show-1 failed with:
                        Error: Directory Server not available.
13.Dec.2013_16:37:47: POK 2.(getSUK) Local-AE-Show-1 failed with:
                        Error: Directory Server not available.
13.Dec.2013_16:37:58: POK 3.(getSUK) Local-AE-Show-1 failed with:
                        Error: Directory Server not available.
```

The next two state logs indicate that the problem is ongoing because all retries have failed, and that the DirX Directory restart recovery operation will be performed:

```
13.Dec.2013_16:38:09: NOK (getSUK) Local-AE-Show-1 failed 3 times
with:
                        Error: Directory Server not available.
13.Dec.2013_16:38:09: NOK local DSA unresponsive - Restarting DirX
will get invoked now (120)
```

The numbers in parentheses (120) in the example above) represents the return code of the script function to be called. This information is used for debugging purposes only and can be ignored in production environments.

The final state log in this series indicates that the restart was successful:

13.Dec.2013_16:38:36: OK (DirXrestart) 1.DirX-Start and LDAP connectivity passed

See the section "Monitoring DirX Directory with the Supervisor" in the *DirX Directory Administration Guide* for additional examples of Supervisor monitoring and recovery operations and state log output during these operations.

1.1.5. Email Client Logging

When email client logging is enabled, the Supervisor calls a mail client in order to send state logs in email messages to the recipient identified in the **toAddr** parameter in **setup_common_data.tcl** over the specified SMTP gateway (the **SMTPserver** parameter in **setup_common_data.tcl**).

On Windows platforms, the email client program **bmail.exe** is a prerequisite for this function.

On Linux platforms, the built-in client **mailx** is called.

The *email* argument to the **dirxsupervisor.tcl** script controls the type of Supervisor state logs that trigger an email notification according to their severity, from critical-only (**1**) to informational (**3**).

1.2. dirxsupervisor

1.2.1. Synopsis

dirxsupervisor [*opMode* [*email* [*verbose*]]]

1.2.2. Purpose

Starts the DirX Directory Supervisor core script (**dirxsupervisor.tcl**) that monitors and repairs the connectivity between a supplier (master)/consumer (shadow) pair of directory system agents (DSAs) in a floating master replication configuration.

1.2.3. Arguments

opMode
Whether (**1**) or not (**0**) the script performs an emergency **dirxadm sob switch** operation to a consumer DSA when it detects an unresponsive supplier DSA. A value of **-1** invokes the "monitoring-only" run mode - in this case, no recovery (neither DirX Directory restart nor DirX Directory emergency switch) is performed at all. This "simulation mode" is helpful for testing the setup parameters in advance. - The default value is **0**.

email
Whether(**1**, **2** or **3**) or not (**0**) the script sends email messages about its monitoring and recovery operations to a Windows email client. To enable email notification, specify the values **1**, **2** or **3**, where each value indicates the severity level of operations that will trigger notification. A value of **1** sends notifications about critical incidents, like emergency switches, disabled shadowing operational bindings, and continuous **ping** and DirX Directory service restart failures. A value of **2** triggers notification on level **1** incidents plus additional warning-level incidents. A value of **3** triggers notification on level **1** and **2** incidents plus additional non-critical incidents, like successful operations. The default value is **0**.

verbose
Whether (**1**) or not (**0**) the script displays progress information during its operation. The

default value is **0**.

1.2.4. Description

The **dirxsupervisor** is a tool that system administrators can run on a DSA to monitor and manage the connectivity between a supplier DSA and consumer DSAs operating in a floating master replication configuration.

The **dirxsupervisor** command processes the password contained in the file (**adm_pwd**) and starts the DirX Directory Supervisor core script (**dirxsupervisor.tcl**).

The **dirxsupervisor.tcl** script makes calls to the other scripts in the Supervisor suite as necessary during its operation.

An instance of the **dirxsupervisor** must be running co-located with each DirX Directory service instance (DSA and LDAP server) in the floating master configuration.

1.2.5. Configuring dirxsupervisor

Use the **setup_common_data.tcl** script to configure **dirxsupervisor** operation.

1.2.6. Invoking dirxsupervisor

Invoke a **dirxsupervisor** session with for example:

```
dirxsupervisor 1 1
```

To set up **dirxsupervisor** monitoring, invoke the DirX Directory Supervisor on each DirX Directory service running in the floating master configuration. It is recommended that you invoke the **dirxsupervisor** on the master/supplier service first.

On startup, the script selects a consumer DSA to monitor based on its position in the cooperating DSA table and identifies this DSA in its startup output.

1.2.7. Terminating dirxsupervisor

The **dirxsupervisor** runs continuously. The **dirxsupervisor** tool stops the scripts on receipt of a signal SIGINT; to terminate it, press CTRL/C.

Make sure you terminate the **dirxsupervisor** before you manually shut down the DirX Directory service on a supplier DSA; for example, to take it offline for maintenance.

1.2.8. Exit Codes

The **dirxsupervisor** command returns an exit code of **0** on success or a non-negative error code if it encounters an error. The text of the error message is displayed on **stderr**.

1.2.9. Examples

The following command sequence starts **dirxsupervisor** with its default values (emergency switch disabled, email notification and verbose mode disabled):

```
dirxsupervisor
```

The following command sequence starts **dirxsupervisor** with emergency switching and email notification enabled:

```
dirxsupervisor 1 1
```

The following command sequence starts **dirxsupervisor** with emergency switching disabled and email notification enabled:

```
dirxsupervisor 0 1
```

The following command sequence starts the **dirxsupervisor** without any recovery enabled and email notification enabled:

```
dirxsupervisor -1 1
```

The following command sequence starts the **dirxsupervisor** while both recovery and email notification remains disabled - also called the simulation mode.This is helpful for testing the setup parameters in advance.

```
dirxsupervisor -1
```

1.2.10. See Also

dirxadm, **dirxcp**, **sob** in the *DirX Directory Administration Reference*, chapter "Monitoring DirX Directory" and chapter "Creating a Shadow DSA" in the *DirX Directory Administration Guide*.

1.3. Supervisor Setup Script

setup_common_data.tcl

1.3.1. Purpose

The Supervisor setup script, used by **dirxsupervisor.tcl**, defines the operating parameters for the DirX Directory Supervisor scripts.The settings in the setup script apply to all

Supervisor instances running in a floating-master configuration.

1.3.2. Description

The default location for the Supervisor script **setup_common_data.tcl** is:

install_path/**monitoring/supervisor**

In the configuration file, comment lines begin with the hash tag character (**#**) in the first column and are ignored. The format of all other lines is:

set *keyword value*

Keyword string values must be enclosed in double quotation marks (").

The following parameters (*keyword*) must be specified:

lang
The operating system language setting. Values are **"German"** or **"English"**.

routerIP
The IP address of a network router in the floating master configuration or the hostname or IP address of one of the DirX Directory service hosts in the floating-master configuration. Specify the IP address in dotted decimal notation; for example, **"123.456.78.910"**.

The specified router must be able to receive **ping** commands.

contextPrefix
The shadowed context prefix in the floating master configuration. The specified context prefix must represent the entire DIT (this is a requirement of a floating-master scenario).

Specify **contextPrefix** in LDAP distinguished name syntax; for example, **"o=my-company,c=de"**. For details about LDAP distinguished name syntax, see the section **Distinguished Names** in the chapter **DirX Directory String Representation for LDAP Binds** in *DirX Directory Syntaxes and Attributes*. For details about shadowed context prefixes, see the chapter "Setting up a Shadow DSA" in the *DirX Directory Administration Guide*.

SVuser
The user that performs **dirxcp** and **dirxadm bind** operations on the Supervisor scripts' behalf and that is also the target of Supervisor script heartbeat checking operations if the optional **testentry** parameter is not specified in the setup script.

SVuser specifies the account that the Supervisor scripts are to use for **dirxadm** binds to the DSA to perform operations such as **sob show** and **sob switch** and for **dirxcp** binds to perform heartbeat checks.

The specified **SVuser** must be an ordinary LDAP user entry. It must be specified in the DirX Directory Administrators (DADM) operational attribute of the root DSE of all DSAs in the floating master configuration so that it is authorized for **dirxadm** binds. For more information on the DADM attribute, see the chapters **DirX Directory Attributes** in *DirX Directory Syntaxes and Attributes* and **DirX Directory Default DSA Schema** in the *DirX Directory Administration Reference*.

If **testentry** differs from the specified **SVuser**, the heartbeat check operation uses **SVuser** for its bind and **testentry** for its modify/read operations.

If **SVuser** is to be used as the heartbeat test entry, it must have a **description** attribute and it must exist in the replicated part of the DIT; otherwise, the update to the **SVuser** entry won't be replicated and a replication problem will be logged.

Specify **SVuser** in LDAP distinguished name syntax; for example, **"cn=supervisor,o=my-company,c=de"**. For details about LDAP distinguished name syntax, see the section **Distinguished Names** in the chapter **DirX Directory String Representation for LDAP Binds** in *DirX Directory Syntaxes and Attributes*.

ldapPort
The TCP port number(s) on which the DirX Directory LDAP server selected to handle Supervisor monitoring requests listens for incoming requests from LDAP clients. The default LDAP port number is **389**. Specify the **ldapPort** parameter once for each LDAP server port you want to identify.

ldapConf
The LDAP configuration subentry for the DirX Directory LDAP server selected to handle DirX Directory Supervisor monitoring requests. Specify **ldapConf** in DAP distinguished name syntax; for example, **"/C=de/O=my-company/CN=ldapconfiguration"**. See the section **Distinguished Names** in the chapter **DirX Directory String Representation for DAP Binds** in *DirX Directory Syntaxes and Attributes*.

The following parameters (keyword) can be optionally specified:

testentry
The entry that is the target of Supervisor script heartbeat checking operations. The specified test entry must be an ordinary LDAP entry, must be located in the replicated part of the DIT, must have a **description** attribute, and must be subject to an ACI-Item that grants add, read and update operations to the specified **SVuser** entry.

Specify **testentry** in LDAP distinguished name syntax; for example, **"cn=supervisor-testentry,o=my-company,c=de"**. For details about LDAP distinguished name syntax, see the section **Distinguished Names** in the chapter **DirX Directory String Representation for LDAP Binds** in *DirX Directory Syntaxes and Attributes*.

If no seperate **testentry** is desired, just assign the **SVuser** (DN) to the **testentry** parameter. In this case the heartbeat check operation uses the **SVuser** entry as the target for its modify or read operation.

opTimeMaxSec
The maximum running time (in seconds) for a heartbeat operation, after which the Supervisor generates a state log message about it – also known as warning-level trigger time.

opCritVal
The maximum running time (in seconds) for a heartbeat operation returning an error – also known as critical-level triggertime.

updtdelaySec
The number of seconds the Supervisor scripts are to wait between heartbeat, ping and Directory service restart operations. The default value is **20** seconds.

retryCnt
The maximum number of times the Supervisor scripts are to retry an operation before logging a notification. The default value is **3**.

retryDelayMsec
The number of milliseconds the Supervisor scripts are to wait between operation retries. The default value is **10000** (10 seconds).

email
Whether (**1**, **2**, or **3**) or not (**0**: default) the Supervisor sends email notifications about monitoring and recovery operations in email messages to a Windows email client and the type of operations (their severity level) that trigger email notification. See the **dirxsupervisor.tcl** reference page for details.

SMTPserver
The SMTP mailbox provider to be used to transfer Supervisor script email notifications to the Windows email client, when this service is enabled. Specify **SMTPserver** in DNS syntax; for example, **"smtp.my-company.com"**.

fromAddr
The address to use in email notifications to identify the sender. Specify **fromAddr** according to the format required by the mailbox provider; for example,
"DirX Directory-Supervisor@my-company.com".

toAddr
The address to use in email notifications to identify the recipient. Specify **toAddr** in according to the format required by the mailbox provider; for example,
"**DirX Directory-Administrator@my-company.com**".

ldapsPort
The LDAP secure port number on which the DirX Directory LDAP server selected for DirX Directory Supervisor monitoring listens for incoming Secure Socket Layer (SSL) requests, or a value of **0** if secured LDAP is not used. A value greater than 0 in this parameter directs the **dirxsupervisor.tcl** script to use a secure LDAP connection the next time it starts.

1.3.3. Example

```
# ##################
# Mandatory settings
# ##################

#set lang "German"
set lang "English"

# router IP
```

```
set routerIP  "192.168.88.130"

# DAP, RPC, LDAP bind specs

set contextPrefix    ",O=My-Company"
set contextPrefix500 [LDAP2DAP $contextPrefix]
set SVuser           "cn=admin$contextPrefix"
set admin500         "${contextPrefix500}cn=admin"

# Test entry to be created - Note: DN expected to be case-sensitive
here !!

set testentry "ou=Heartbeat,$contextPrefix"
#set testentry "$SVuser"
set ldapPort         19001
set ldapPort         389
set ldapsPort        0
set ldapConf         CN=ldapConfiguration

# #################
# Optional settings
# #################

# Expected Modify runtime at maximum for warning
set opTimeMaxSec     10
set opTimeMaxUsec    [expr $opTimeMaxSec * 1000000]
# Expected Modify runtime at maximum for critical
set opCritVal      [expr $opTimeMaxSec * 2]
# Delay between heartbeat / ping / DxD restart probes
set updtdelaySec     10
set updtdelayMsec    [expr $updtdelaySec * 1000]
# Repetition rate of the Heartbeat-Operation before escalation
set retryCnt           3
# Repetition delay on unexpected operational behavior
set retryDelayMsec 10000

# SMTP mail parameters

  set SMTPserver  "email.my-company.com"
  set fromAddr    "Gunter.Katt@my-company.com"
  set toAddr      "Gunter.Katt@my-company.com"
```

1.4. Supervisor Password File

adm_pwd

1.4.1. Purpose

The password associated with the account specified in **SVuser**.This is the password the Supervisor scripts will use during **dirxcp** and **dirxadm** bind operations.

1.4.2. Description

The default location for the password file **adm_pwd** is:

*install_path***/monitoring/supervisor**

The password is the only content of this file. The password is associated with the account specified in **SVuser**. It is the password the Supervisor scripts will use during **dirxcp** and **dirxadm** bind operations.

When creating the file, the password must be specified in plain ASCII format. Once the Supervisor has accessed the file one time, it changes the content to the encrypted format of the password and reuses the encrypted format in subsequent starts.

It is strongly recommended to protect the password file by means of the operating system so that access is only granted to the Supervisor process.

1.4.3. Example

```
dirx
```

DirX Product Suite

The DirX product suite provides the basis for fully integrated identity and access management; it includes the following products, which can be ordered separately.

DirX Identity

DirX Identity provides a comprehensive, process-driven, customizable, cloud-enabled, scalable, and highly available identity management solution for businesses and organizations. It provides overarching, risk-based identity and access governance functionality seamlessly integrated with automated provisioning. Functionality includes lifecycle management for users and roles, cross-platform and rule-based real-time provisioning, web-based self-service functions for users, delegated administration, request workflows, access certification, password management, metadirectory as well as auditing and reporting functionality.

DirX Directory

DirX Directory provides a standards-compliant, high-performance, highly available, highly reliable, highly scalable, and secure LDAP and X.500 Directory Server and LDAP Proxy with very high linear scalability. DirX Directory can serve as an identity store for employees, customers, partners, subscribers, and other IoT entities. It can also serve as a provisioning, access management and metadirectory repository, to provide a single point of access to the information within disparate and heterogeneous directories available in an enterprise network or cloud environment for user management and provisioning.

DirX Access

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy- and risk-based authentication, authorization based on XACML and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including FIDO, identity federation based on SAML, OAuth and OpenID Connect, just-in-time provisioning, entitlement management and policy enforcement for applications and services in the cloud or on-premises.

DirX Audit

DirX Audit provides auditors, security compliance officers and audit administrators with analytical insight and transparency for identity and access. Based on historical identity data and recorded events from the identity and access management processes, DirX Audit allows answering the “what, when, where, who and why” questions of user access and entitlements. DirX Audit features historical views and reports on identity data, a graphical dashboard with drill-down into individual events, an analysis view for filtering, evaluating, correlating, and reviewing of identity-related events and job management for report generation.

For more information: support.dirx.solutions/about

Legal remarks

On the account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Eviden sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available locally. The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Eviden reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Eviden sales representative for the most current information. Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.