Evidian

DirX Directory V8.7

High-End Directory Server

High-performance, highly available, highly reliable and secure LDAP and X.500 directory server and LDAP proxy

Directory services are critical components of today's highly interconnected business environment, providing the foundation for identity and access management across the ever-widening boundaries of the enterprise. In the intranet environment, the directory service provides a global repository for shared information about employees, organizations, and resources such as applications, network devices, and other distributed services, accommodating hundreds of thousands of users. In the extranet environment, the directory service maintains profile information about customers, trading partners, and suppliers, holding millions of users. For both environments, the directory service must be able to manage user identities and control access to the information and services offered to its users, and it must provide fast, always available, authenticated access to the information and services, potentially to a huge number of users.

DirX Directory meets these requirements, and more. The DirX Directory service provides a standards-compliant, high-performance, highly available, highly reliable identity management platform with near-linear scalability. DirX Directory can act as the identity store for employees, customers, trading partners, subscribers, and other e-business 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.

Standards and compatibility

DirX Directory implements the LDAPv3 and X.500 directory standards. DirX Directory permits third-party LDAP-enabled applications to manage the directory schema over LDAP. DirX Directory runs on the most popular operating systems and supports a wide variety of applications via the Lightweight Directory Access Protocol (LDAP).

High performance

DirX Directory is based on the innovative DBAM database kernel (Directory Basic Access Method) that is optimized for directory access, allowing sub-second response times and high throughput rates for parallel queries.

High availability and reliability

To meet reliability requirements for the directory service, DirX Directory supports floating master replication for high availability configurations (a software solution instead of adding hardware clusters) and failover. For backup and recovery, DirX Directory supports full and differential saving in parallel with directory update operations. Transaction processing in the database provides guaranteed recovery after crashes without data loss.

Identity management

As the foundation for an identity management system, DirX Directory can manage user and subscriber profiles, digital certificates for public key infrastructures (PKIs), authorization and authentication information, access permissions and other relevant attributes for users and subscribers that control access to information, network resources, or distributed services.

Security

DirX Directory supports SSL/TLS for LDAP server and client authentication, X.500 DAP authentication, authorized user access control, encrypted communication, and server-side policies for local security management. DirX Directory also permits the creation and enforcement of password policies to control how passwords are used and administered in an enterprise network. Policies for password complexity, aging, and reuse after expiration are supported. High performance audit is provided for traffic analysis and accounting.

Scalability

The DBAM database kernel is designed to permit linear scalability in a single directory server. Benefits: DirX Directory can accommodate future growth on existing hardware configurations, can scale rapidly to store huge number of users in an extranet or cloud deployment and can scale from workgroup to enterprise to e-business directory roles.

Running the DirX Directory LDAP Server in proxy mode provides a central access point to a directory service for LDAP clients, and extends both scalability and availability.

Administration

DirX Directory offers powerful graphical and command-based scriptable tools for centralized administration of a distributed directory system, including auditing, monitoring, and logging functions.

Access to DirX Directory

The data stored in DirX Directory is accessible through

- Any LDAP client and LDAP-enabled application
- A command-line administration interface with full LDAP functionality which can also be controlled via Tcl scripts
- DirX Manager, a Java-based management client

DirX Directory components

- Directory System Agent DSA
- LDAP server and LDAP proxy
- Java-based, graphical administration interface **DirX Manager** for configuration and administration of local and remote DirX Directory servers
- Command-driven bulk-loading tools **dirxload** and **dirxmodify**
- Command-driven directory client **dirxcp** for the administration of entries via LDAP and DAP
- Command-driven management client **dirxadm** for DSA and LDAP servers
- Command-driven backup and restore tool **dirxbackup**

Directory protocols

The following protocols are supported in accordance with the Internet and 1993 X.500 standard:

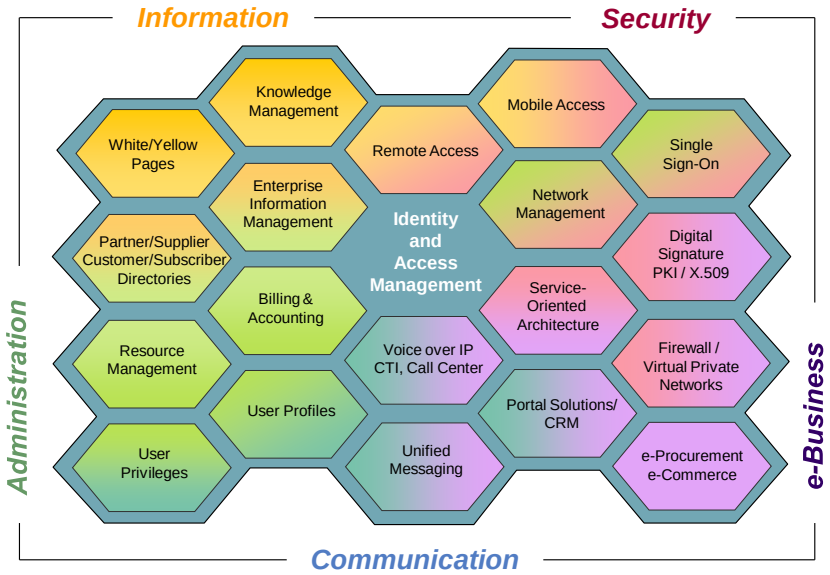
LDAP: The Lightweight Directory Access Protocol, the Internet directory standard, is supported efficiently by an integrated LDAP server.

DAP: The Directory Access Protocol, which defines the exchange of queries between Directory User Agents (DUA) and Directory System Agents (DSA).

DSP: The Directory System Protocol, allowing DSAs to forward queries and administration requests they cannot answer themselves to other DSAs. This protocol also handles returning of results to the DSA where the search query or request originated.

DISP: The Directory Information Shadowing Protocol provides for data replication between DSAs. As the protocol also regulates copying of the access control data, collective attributes and schema information, replicated data can be accessed without loss of information.

IDM: The Internet Directly Mapped (IDM) protocol is a mapping of the X.500 protocols directly onto TCP/IP and is supported for DAP, DSP and DISP.



DirX Directory – Areas of application

X.500 information model

DirX Directory conforms to the information model of the 1993 X.500 standard and supports, among others:

- Collective attributes - identical attributes of several directory entries which are accessed like normal attributes but which are stored once only and managed at a central location
- Access control rules for parts of a directory tree
- Attribute subtyping; the option of accessing specific attributes by referencing generic attributes (e.g., PrivateTelephoneNumber as a subtype of TelephoneNumber)
- Operational attributes; attributes used for internal purposes or which, like the timestamp, are generated by the directory itself.

Directory schema

DirX Directory supports the attribute types and syntax rules defined in X.520.

The attribute types defined in X.509 and the matching rules defined in X.521 are also supported, as are phonetic rules for finding entries with similar values.

Likewise supported are all object classes defined in X.521 as are all object classes, attribute types and syntaxes defined by LDAP RFCs 4512, 4517, 4523 and 2798 (inetOrgPerson).

DirX Directory allows storing X.509 attribute certificates by providing support for X.509 (2000) attribute certificate syntax.

DirX Directory supports the ACP 133 schema in accordance with the document "Common Directory Services and Procedures Supplement ACP 133 SUPP-1(A)" by the Combined Communications Electronics Board (CCEB).

In extension to the X.500 standards and LDAP RFCs, DirX Directory supports dynamic groups and multi-level nested groups. Various attributes are provided to support LDAP applications in identifying and resolving dynamic and nested group memberships. DirX Directory allows using dynamic and nested groups for the management of access control and user policies.

The LDAP server supports the attributes of the LDAP root DSE as defined by RFC3045 and RFC4512.

DirX Directory supports schema management over standard LDAPv3 clients like DirX Manager or the bulk-loading tool dirxmodify.

It allows both the handling of standardized schema elements and the definition and administration of private object classes and attributes.

DirX Directory also allows enforcing the uniqueness of attribute values for specific attribute types (e. g., with string syntaxes) within the directory server and all its full shadows.

LDAP server and LDAP proxy

DirX Directory includes an LDAPv3 server, which provides access from any LDAP client.

The LDAP server is a full implementation of the core LDAPv3 protocol.

The LDAP server may be installed co-located with the DSA or on a remote system.

For load balancing one can connect more than one LDAP server with a DSA and one LDAP server can be connected to multiple DSAs if they are full shadow DSAs. In the latter case, LDAP clients might benefit from the implemented failover mechanism as in most cases the LDAP client operations can still succeed even if one DSA cannot serve the request.

The LDAP server supports secure communication over SSL/TLS.

The LDAP server supports a configurable, high-performance result cache with selective update that is well-suited for high-performance applications.

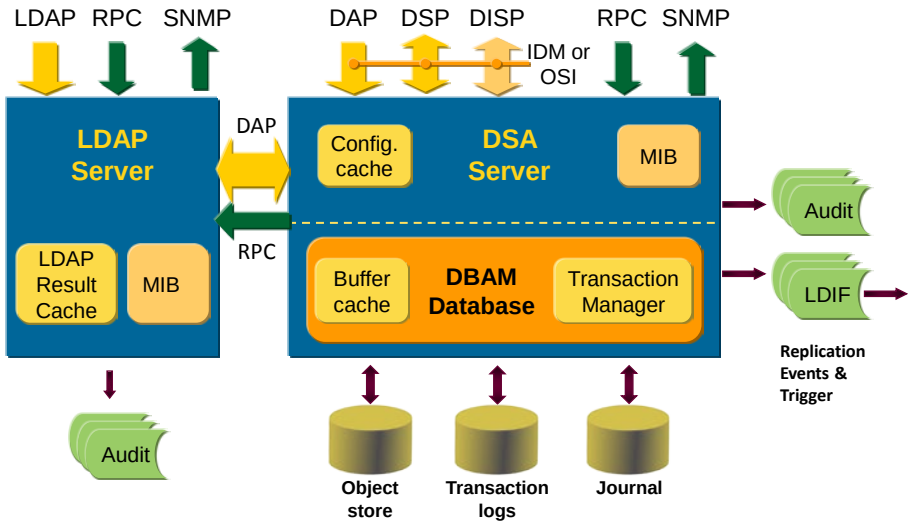
LDAP Proxy

Running the DirX Directory LDAP server in proxy mode allows routing incoming LDAPv3 requests from LDAPv3 clients to any remote target LDAPv3-compliant directory server and associates responses back to the requesting client.

The main advantage of an LDAP proxy is to provide a central access point for LDAP clients hiding the actual processing server knowledge from them as well as hiding server outages from clients and providing load balancing transparently to the clients.

Key features of the DirX Directory LDAP proxy include:

- Rule-based request routing: The LDAP Proxy selects the target server based on the evaluation of a configurable set of rules. Both user-routing rules and operation-routing rules are supported.
- Load Balancing: A round-robin mechanism selects the target server for the next connection to be routed to, taking into account the results of the rule evaluation of the request routing.
- Failover: If a target server is unavailable due to connection error, the request fails over to the next appropriate target server according to configuration settings.
- Rule-based LDAP request and result rewriting: The rewriting feature includes schema and attribute mapping to provide schema compatibility that is helpful for clients that use an outdated schema or that contain a hard-coded schema.
  This feature can also be used to implement an additional access control layer. One can define what actions users are allowed to do by denying certain requests or hiding or blocking critical subtrees, entries and attributes of search operations and their results. It also allows protecting the directory infrastructure from specific end users.



DirX Directory - Architecture

DBAM data management

The data management of DirX Directory builds on the innovative DBAM database kernel, which offers a highly efficient basis for virtually unlimited scalability, optimum access and directory tree modelling.

Key advantages of the database include:

- Huge storage capacity
- Optimum indexing for fast, efficient search operations
- High-performance name resolution and name retrieval
- High-performance database cache for buffering portions of the directory data in main memory
- High-performance transaction handling and recovery
- Support of LDAP RFC 2696 for high-performance paged results

For the management of the DBAM database, DirX Directory provides utilities for:

- Configuring the DBAM database
- Checking the DBAM database
- Post-indexing of attributes
- Reorganizing the database to provide optimized access
- Recovering (saving and restoring) the database

LDIF

DirX Directory supports high-performance export to LDAP Data Interchange Format (LDIF) files. One can flexibly export the whole DSA database or parts of it (LDIF content files) or just changes to the existing data (LDIF change files). This permits administrators to carry out bulk data transfers and to integrate DirX Directory with other directories and especially to use it as a metadirectory store. LDIF files provide the interface to publish directory change events. Post-processing of LDIF files can be triggered automatically.

Replication

DirX Directory implements the creation and automatic update of directory replicas (shadows) in order to increase data availability and access performance.

In a replication environment, a master DSA replicates data to one or more shadow DSAs. For high-availability, DirX Directory supports the floating master concept, where a shadow DSA can act as the new master DSA if the old master DSA has a failure.

Each shadow DSA can be set up to work either in synchronous or asynchronous shadowing mode.

Because it ensures data synchronicity, a synchronous shadow DSA is an ideal candidate for load distribution purposes and failover in the floating master scenario.

A synchronous shadow DSA is also suitable for LDAP/DAP clients that perform read operations immediately following successful modify operations: whenever an LDAP client reads after a successful modify operation, it receives the right result.

In contrast to synchronous shadowing, which always replicates the entire master directory tree, asynchronous shadowing provides greater flexibility in defining the replication area according to selected attributes or the parts of the tree to be replicated.

DirX Directory DSAs support a number of shadowing options:

- Incremental-refresh and total-refresh operations over DISP
- Periodic update and update on change over DISP
- High-performance bulk replication based on save and restore of the database for total refresh

Distribution

Scalability, availability, load distribution and performance tuning are the main reasons to set up a distributed directory service. DirX Directory supports a number of options to set up a distributed directory service:

- Distributed directory service based on shadowing, where one master DSA holds the complete Directory Information Tree (DIT) and shadow DSAs hold replicas of the DIT
- A true distributed directory service, where the DIT is split over different DSAs
- A combination of true distribution and shadowing in which pieces of a DIT held by two different DSAs are replicated to each DSA
- LDAP and DSA servers can be deployed on different machines and multiple LDAP servers can be connected to one DSA server

DSAs communicate over DSP to provide a seamless view of the distributed directory service to applications.

Security

DirX Directory supports the SSL/TLS (Secure Socket Layer 3.0 / Transport Layer Security 1.0/1.1/1.2) protocols creating the basis for authenticated, encrypted communications via the Internet for:

- LDAP servers and LDAP clients
- X.500 DAP, DSP and DISP for X.500 DSA-to-DSA and DUA-to-DSA communication over IDM.

In addition, DirX Directory supports:

- Authentication between DUA and DSA by means of the DAP protocol or between servers by means of server-server protocols,
- Access control in order to restrict access to authorized users and
- Server-side policies for local security management.

Authentication

For authentication over LDAP, a series of security layers can be used, depending on concrete needs:

- Simple bind using name and password
- Simple bind using name and password via an encrypted connection over SSL/TLS
- SASL authentication with mechanism EXTERNAL (certificate-based SSL/TLS client authentication)
- Configurable support of external authentication for LDAP simple binds using Microsoft Windows or LDAPv3, e.g. to an IBM RACF LDAP server.

DirX Directory leverages certificate revocation lists (CRLs), i.e. a revoked certificate from a given CRL is no longer useable for a successful SASL authentication.

DirX Manager provides authentication/login via CardOS smart cards that are supported by Atos CardOS API. From the LDAPv3 protocol view, smart card login maps onto an LDAP SASL bind with the mechanism type EXTERNAL. This means the security services of the underlying TLS/SSL layer are used to perform the client authentication that is based on strong cryptography.

Access control

Access to DirX Directory information is protected in a number of ways and can be defined down to the level of individual attributes in entries. DirX Directory supports both Basic Access Control (BAC) and Simplified Access Control (SAC) including Access Control Information for entries, sub-entries and attributes.

As an extension to the X.500 model, both the access control targets and the affected users can be defined by arbitrary LDAP filters.

The model of proxied authorization is supported according to RFC 4370.

The auditing functionality enables system security to be monitored and documented.

Password Policies

To enhance the directory security, DirX Directory allows defining and enforcing password policies. Password policies control how passwords are used and administered in an IT system. They provide a set of rules that ensure that

- Passwords meet construction requirements to prevent users from choosing easy-to-guess passwords (Password Check Syntax, Password Minimum Length, Password Maximum Length, Password Minimum Special Characters, Password Minimum Lower Case Characters, Password Minimum Upper Case Characters, Password Minimum Numeric Characters, Forbidden use of sub/super-string of RDN as password),
- Users change their password periodically (Password Minimum Age, Password Maximum Age, Password Expire Warning, Password Grace Login Limit),
- The re-use of old passwords is restricted (Password In History, Password Must Change) and
- Accounts are locked out after failed logins (Password Lockout, Password Lockout Duration, Password Maximum Failure, Password Failure Counter Interval).

They also provide information about level and algorithm of password hashing (password storage scheme, password storage scheme level) and control the operational attributes for last login time and number of failed logins.

Supported password storage schemes: plain, hashed, salted-hashed.

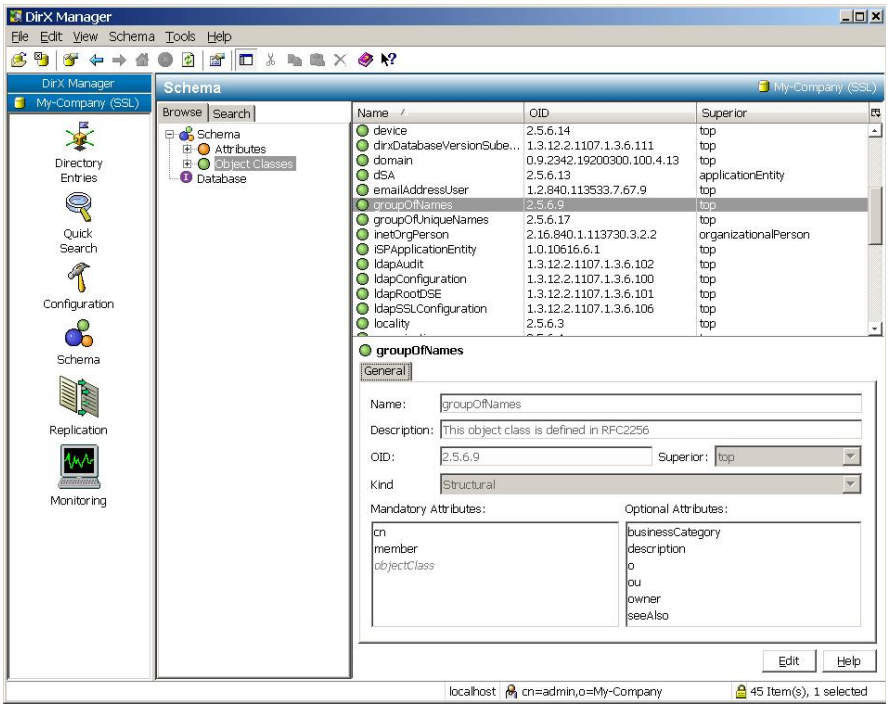
Supported password storage hash algorithms: SHA-1 and SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512).

To support the password policy procedures specified by the password policy, each user entry contains a set of operational attributes that provides information about the current status of the user's password. This set of attributes provides state information to support procedures for

- Password checking
- Password aging
- Account lockout
- Password administration

Public Key Infrastructure Support

DirX Directory supports the X.509V3(97) standard for secure management of public key certificates. As a result, the storage of certificates and revocation lists, which can be



DirX Manager Sample – Schema Management

produced by Certification Authorities (CAs), is also supported. DirX Directory has been successfully tested with products from leading CA vendors.

Audit Logging

The purpose of audit logging is to record information about interactions with the directory for subsequent use. Recorded information is configurable and includes:

- The session ID to identify the connection
- The protocol used to access the server
- The identity of the user, if known
- The type of directory operation performed, with a timestamp, duration, and a summary of its arguments.
- The result of the operation or the reason for failure
- Session tracking control values such as source IP, source name

This information is placed in an audit log file, and can be used to analyze traffic or to support billing and accounting management.

Audit logging is supported for all protocols for both the DirX Directory DSA and the LDAP server.

For subsequent analysis, command line tools are provided that allow summarizing and filtering the audit log files according to selected criteria.

DirX Directory MIBs

DirX Directory supports MIB information based on RFC 2605 and RFC 2788 as well as DBAM statistics.

The administrator can monitor the MIB information of both the DSA and LDAP server by using the dirxadm tool or DirX Manager.

SNMP Support

DirX Directory supports the sending of SNMPv2 traps according to the RFC1155 and RFC1905 standards.

Administrators use a configuration file to set up and enable SNMP operation.

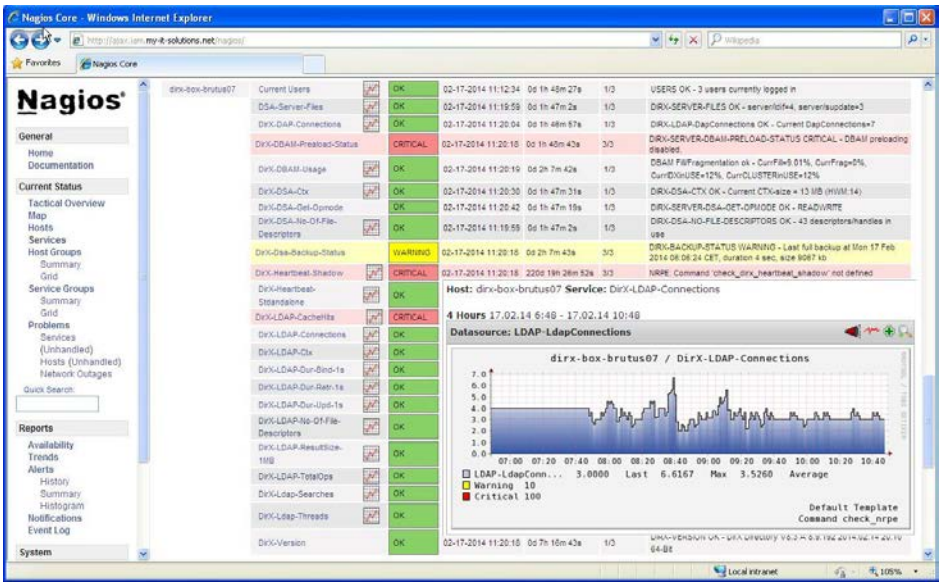
Monitoring the directory service with SNMP traps can help to detect critical situations prior to a severe incident, e.g., lack of resources.

Nagios Support

DirX Directory provides a set of specialized Nagios plugins that can be used in an existing Nagios environment to monitor the status of DirX Directory service resources and operations and collect statistics about these items for later performance analysis.

The DirX Directory Nagios plugins allow to monitor:

- Resources consumed by DirX Directory processes, such as memory allocation and file descriptors
- The responsiveness of DirX Directory processes (the DSA and LDAP servers) running in standalone and replication configurations



DirX Directory - Nagios Integration Sample

- Resource and operational statistics kept by the LDAP server in its MIBs and the changes to these counters over time
- Result sizes returned by LDAP search operations and the duration of LDAP client calls
- The frequency of DirX Directory database backup operations
- The capacity of DBAM devices configured in a DirX Directory installation
- The operational status of the DBAM database
- The operating mode of the DirX Directory service

The DirX Directory Nagios plugins provide input parameters for specifying warning and critical thresholds to be monitored for DirX Directory service operations, offering DirX administrators the opportunity to respond to problems detected by the plugins and displayed by the Nagios server before they become severe, and to track their resolution.

The DirX Directory Nagios plugins are delivered as full-function Perl-based executables that can be extended to address customer-specific DirX Directory monitoring requirements

High-availability configuration

DirX Directory is intended to operate in environments where availability, scalability and performance are of utmost importance.

Delivering such a platform requires either a software-based solution or a combined, integrated hardware and software solution.

As a software solution, one can use the DirX Directory replication functionality. DirX Directory allows implementing a floating-master concept by supporting manual and automated mechanisms to easily switch a full shadow server to a master server, providing a continuous service for both read and write operations.

As an alternative or an addition to a software-based high-availability strategy, one can also use a combined, integrated hardware and software solution. While there are various configurations for such a solution, three components are of central importance:

- A two-node cluster system
- A RAID system connected to both nodes
- An uninterruptible power supply (UPS) or similar computer center functionality

Cluster systems are a technology that connects a number of nodes (servers) to a single system image to provide continuously available systems. Clusters are configured without any point of failure, including network, cluster interconnect, storage and software. Cluster applications like DirX Directory can be implemented as a failover service: the cluster automatically relocates the application in the event of node failure. Not every failure has to lead to a node failover: application watchdogs and other services may recover on the same node. The stand-by node can be used for load distribution and performance enhancement (by a DirX Directory copy or another application) as long as the primary node is running.

RAID (Redundant Arrays of Independent Disks) is a technology used to improve data protection and performance while storing large amounts of data. RAID level 10 is the one recommended for the DirX Directory configuration. RAID level 10 is a combination of level 0 (data striping over more than two drives, which dramatically improves performance) and level 1 (data mirroring, where data are copied automatically to a second set of drives, offering good data protection and fast recovery). In addition, the mirror disks contribute to the performance by doubling the read throughput.

Supervisor

Automated switching in a floating-master configuration is supported by the script-based DirX Directory Supervisor that provides for

continuous, periodic monitoring on replication and network connectivity level between the DirX Directory service instances. The Supervisor scripts can be customized to adjust the triggering conditions for switching a full shadow server to a master server automatically.

Scalability

DirX Directory has a highly scalable architecture regarding both the number of entries it can store and the number of concurrent users and queries it supports.

Database scalability:

- One server can store and manage tens of millions of entries, including all the necessary indices.
- An unlimited number of entries can be stored below one single node.
- For optimal storage of large attribute values, outsourcing of attributes is supported.
- For unlimited scalability, several servers can be connected to set up a distributed directory system. The complete data of all connected DirX Directory servers is accessible for read and write operations.

User queries and throughput scalability:

- Optimized indexing for fast and efficient search operations
- Multi-level caching, automatic cache preload and tuning of cache sizes
- Multi-threaded server architecture provides linear scalability based on the number of processors
- Use of high-performance disk subsystem (e.g., RAID 10) or SANs
- Load distribution based on replication and distribution of data to multiple servers
- Multi-version DBAM to optimize throughput during update operations, allowing one update operation and multiple retrieval operations in parallel
- LDAP and DSA servers can be deployed on separate machines
- Multiple LDAP servers can be connected to one DSA server or one LDAP server can be connected to multiple DSAs for optimal load distribution.

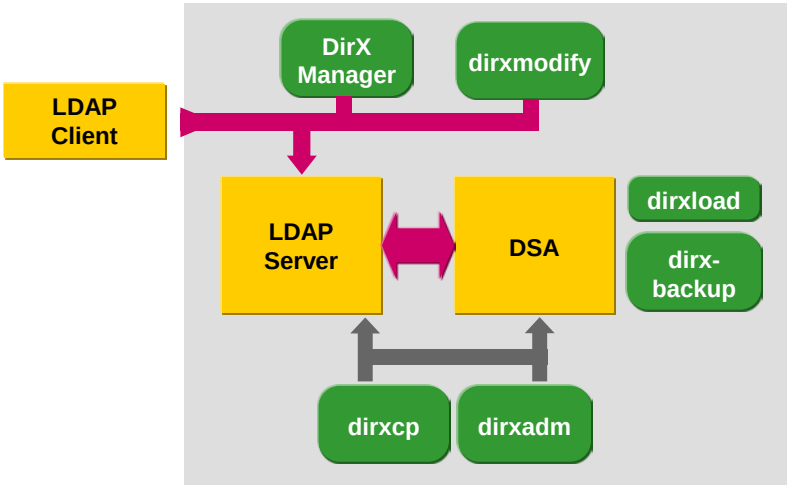
Administration

DirX Directory provides a number of administration tools:

The dirxload component is a high-performance bulk-loading tool used to load large amounts of data off-line directly into the database.

The dirxmodify component is a bulk-loading and checking tool that operates over LDAP.

The dirxadm/dirxcp components and the DirX Manager graphical interface are used for DirX Directory administration. dirxcp and dirxadm are based on the shell-like command language Tcl (Tool Command Language). Tcl supports the use of variables, conditional statements, list-processing functions, looping and other features of well-known command languages. These features permit the implementation of



DirX Directory - Administration

shell scripts for batch processing, and consequently allow simple system customizing.

The dirxcp/dirxadm programs supplement these functions by providing predefined commands for the management of DirX Directory administration objects and for simplifying the routine tasks of the DirX Directory administrator.

The dirxadm/dirxcp tools can be used in two different modes:

- In interactive mode, in which individual commands are entered in a dialog and results are displayed
- In command mode, in which whole series of commands can be executed.

The dirxbackup program is a command-line tool for saving and restoring the DBAM database to and from a DBAM database archive.

The dirxload component

The dirxload component is an off-line bulk-loading tool used to load large amounts of data in an optimized and efficient way. This bulk-loading tool can be used for initial loading, populating the database or for subsequent additions to the database. The administrator can specify one or more LDIF content files to load directly into a DBAM database. Optionally, dirxload can be configured to perform attribute indexing during the load operation.

The dirxmodify component

The dirxmodify component processes LDIF content or change files and performs the modifications over LDAPv3 to the directory database. It is a stand-alone tool that can be run locally or from a remote machine. dirxmodify is a very powerful tool with many on-the-fly processing options that can also be used off-line for checking LDIF files and generating statistics.

In particular, dirxmodify:

- Supports anonymous and simple authenticated bind to the LDAP server
- Converts ISO-8859-1 (Latin-1) characters to UTF-8 characters
- Checks the LDIF files off-line for syntactical correctness and displays statistics about attributes, entries, and nodes in the file
- Performs simple queries directly on the LDIF file
- Replaces attribute values and types on-the-fly from the file into the directory
- Ignores selected attributes for loading

The dirxcp component

The dirxcp tool is a command-driven directory client that can be used by administrators or users to communicate with an LDAP server over LDAP or directly with a DSA over DAP. It is used to:

- Send requests to DSAs to perform operations such as generate new objects, change, delete, and search for objects/entries in the directory information tree (DIT),
- Execute queries on objects in the DIT,
- Change parameters in order to change the behavior of operations and
- Display abbreviations used for attributes and object identifiers.

The dirxadm component

The dirxadm tool is a set of commands that allow the system administrator to manage LDAP servers and DSAs; for example, DSA-specific entries (DSEs) and operational attributes.

The commands are used to:

- Manage the local DSE and DSA policies
- Manage the links between two DSAs (operational bindings for replication events and distribution of directory data among two DSAs)
- Configure the DSA database
- Display monitoring information stored in the Management Information Base of the DSA
- Perform administration tasks such as
  - Starting/terminating the servers and
  - Enabling/disabling logging.

The dirxbackup component

DirX Directory provides full and differential saving without service interruption. Both retrieval and update operations are allowed during the backup.

The dirxbackup tool saves, restores and verifies a DBAM database. The tool can be used in conjunction with a file compress/uncompress tool such as gzip.

The commands are used to:

- Save a DBAM database in a database archive
- Restore a DBAM database from a database archive
- Verify a database archive for consistency

DirX Manager

DirX Manager, a Java-based LDAP management client, provides a configurable, platform-independent graphical administration interface for local and remote administration of DirX Directory.

The main features provided by DirX Manager are:

- Entry management (add, delete, modify)
- Browsing and searching of the directory
- Schema management over LDAP
- Replication management over DirX Directory RPC
- Display of indices
- Management and display of subentry information
- Password policy management
- Proxied authorization control management
- Directory monitoring view for LDAP and DSA over LDAP-extended operations
- Management of multiple servers
- Import from LDIF content and change files and from DSMLv1 and DSMLv2 files into the directory
- Export of selected directory content into DSMLv1, DSMLv2 or LDIF content files
- SSL server authentication
- Customizable logical views
- Setup of scripts and execution of dirxcp and dirxadm in a GUI pane
- Support of simple paging

Logging of system events

DirX Directory offers two levels of program monitoring:

- System error and status reports
- Monitoring of program execution

The administrator can configure which messages are logged, in which form, and where they are stored. On UNIX systems, error and status messages can also be passed to the UNIX syslog daemon.

Integration on Windows platforms

The administration of DirX Directory is adapted to and integrated into the system environment on Windows platforms:

- Display of logging information with the Event Viewer
- DirX Directory runs as a Windows service and can be managed by Windows Service Administration

Support of 64-Bit Architectures

DirX Directory runs as native 64-bit application with Red Hat Enterprise Linux 7, SUSE Linux Enterprise Server 12, and Microsoft Windows Server 2016 on x86-64 architectures (Intel).

Compliance with standards and interoperability

DirX Directory complies with Internet LDAP standards: RFCs 1155, 1274, 1277, 1905, 2222, 2247, 2279, 2377, 2559, 2587, 2596, 2696, 2798, 2849, 2891, 3045, 3673, 4370, 4510, 4511 , 4512, 4513[1], 4514, 4515, 4516, 4517, 4518[2], 4519, 4529, 6171, MIB information based on RFC 2605[3] and 2788[3]

DirX Directory also complies with the following ITU-T and ISO/IEC standards:

ITU-T X.500, X.501, X.511, X.518, X.519, X.520, X.521, X.509, X.525

ISO/IEC 9594-1, 9594-2, 9594-3, 9594-4, 9594-5, 9594-6, 9594-7, 9594-8, 9594-9

1993 profiles:

ADY11, ADY12, ADY21, ADY22,

ADY41, ADY42, ADY43, ADY44,

ADY45, ADY51, ADY53,

FDY11, FDY12

In addition to IPv4, DirX Directory supports IPv6 for the following protocols:

- LDAP
- X.500 DAP/DSP/DISP (IDM-based)

By means of configuration, administrators can choose the IP version supported for incoming traffic and used for outgoing traffic.

Other DirX products

The following products also belong to the DirX product suite and can be ordered separately; DirX provides the basis for totally integrated identity and access management:

DirX Identity provides a comprehensive, process-driven, customizable, cloud-ready, scalable and highly-available identity management solution for enterprises and organizations. It delivers overall identity and access governance functionality seamlessly integrated with automated provisioning. Features include life-cycle management for users and roles, cross-platform and rule-based provisioning in real-time, Web-based user self-service and delegated administration, request workflows, access certification, password management, metadirectory and auditing and reporting.

DirX Access is a comprehensive, cloud-ready, scalable, and highly available access management solution providing policy-based authentication, authorization and federation for Web applications and services. DirX Access delivers single sign-on, versatile authentication including risk-based authentication, 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-premise.

DirX Audit provides auditors, security compliance officers and 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, a monitor for identity-related events and job management for report generation. With its analytical features, DirX Audit helps enterprises and organizations to ensure sustainable compliance and provide business intelligence for the identity and access management processes.

[1] Except Digest authentication

[2] Matching rule implementation according to X.500

[3] Not supported via SNMP but via RPC and LDAP extended operations

System Requirements for DirX Directory V8.7

Hardware

- Intel server platform for Microsoft Windows Server 2016, SUSE Linux Enterprise Server 12, Red Hat Enterprise Linux Server 7

Memory requirements:

- Main memory: minimum 8 GB RAM
- Disk Space: minimum 3 GB plus disk space for data

Software

- Microsoft Windows Server 2016 (Long-Term Servicing Channel) Version 1607 (x86-64)
- Red Hat Enterprise Linux Server 7 (x86-64)
- SUSE Linux Enterprise Server 12 (x86-64)
- Microsoft Windows 7 (x86-64, DirX Manager only)
- Microsoft Windows 10 (x86-64, DirX Manager only)

with the latest patches/service packs for the selected platform

Support of cluster configurations is available on request

Virtual Machine Support:

- VMWare ESXi 6.0/6.5, in combination with guest operating systems listed above that are supported by VMWare ESXi 6.0/6.5

For DirX Manager

- Java SE Runtime Environment 8 (see dependencies on selected operating system)
- For smart card support: Atos CardOS API V5.3/V5.4 in combination with CardOS smart cards that are supported by Atos CardOS API V5.3/V5.4

For Supervisor

- Perl and perl-ldap distribution latest release
  - On Windows: Perl 5.16.3 or newer
  - On Linux: Perl 5.8 or newer

For Nagios integration

- Nagios Core Version 3.4.4
- Perl and perl-ldap distribution latest release
  - On Windows: Perl 5.16.3 or newer
  - On Linux: Perl 5.8 or newer

User interface

English

Documentation

The following DirX Directory documentation is available electronically in PDF:

- Administration Guide
- Administration Reference
- Disc Dimensioning Guide
- External Authentication
- LDAP Proxy
- LDAP Extended Operations
- Manager Guide
- Plugins for Nagios
- Supervisor
- Syntaxes and Attributes
- Guide for CSP Administrators

More information:
www.evidian.com

All trademarks are the property of their respective owners. Atos, the Atos logo, Atos Codex, Atos Consulting, Atos Worldgrid, Bull, Canopy, equensWorldline, Unify, Worldline and Zero Email are registered trademarks of the Atos group. Atos reserves the right to modify this document at any time without notice. Some offerings or parts of offerings described in this document may not be available locally. Please contact your local Atos office for information regarding the offerings available in your country. This document does not represent a contractual commitment. November 2018. © 2018 Atos