

华为 DSM 文档安全管理系统 特性描述

文档版本 05
发布日期 2012-10-25

华为技术有限公司



版权所有 © 华为技术有限公司 2012。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： <http://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 概述	4
1.1 背景.....	4
1.2 产品简介.....	5
1.3 产品特性.....	8
2 体系结构	9
2.1 系统组成.....	9
2.1.1 组成图.....	9
2.1.2 DSM 管理中心.....	11
2.1.3 DSM 服务器.....	13
2.1.4 DSM 客户端.....	14
2.2 配置要求.....	16
2.2.1 服务器配置要求.....	16
2.2.2 客户端配置要求.....	16
3 组网方案	18
3.1 集中式组网.....	18
3.2 分布式组网.....	21
4 功能特性	25
4.1 文档权限管理.....	26
4.2 组策略和权限模板.....	28
4.3 跨系统授权.....	28
4.4 用户漫游.....	29
4.5 文件类型和编辑器.....	29
4.6 对外 API 接口支持.....	30
4.7 日志管理.....	31
4.8 用户和部门管理.....	31
4.9 服务器管理.....	32

1 概述

关于本章

介绍 DSM 产生的背景以及 DSM 产品的特性。

1.1 背景

随着信息化程度的提高，企业越来越多地利用计算机创建和处理敏感的业务电子信息，在方便快捷的同时也增加了信息被侦听、截获及非法拷贝的危险。

1.2 产品简介

介绍 DSM 的主要特点。

1.3 产品特性

介绍 DSM 的主要特性。

1.1 背景

随着信息化程度的提高，企业越来越多地利用计算机创建和处理敏感的业务电子信息，在方便快捷的同时也增加了信息被侦听、截获及非法拷贝的危险。

尤其企业在商业活动中使用的诸如企业财务数据表、客户信息、研发文档、图片等隐私和敏感信息资源，一旦泄密将给公司的业务关系带来危害，使公司的知识产权遭受损失，带来巨大的信息资产损失成本，同时给公司的声誉造成不良影响。

据调查显示，信息泄密已成为当前企业面临的 TOP10 安全威胁之一。在 Fortune 排名 1000 的公司中，平均每次电子文档泄密造成的损失为 \$50 Million，而不受权限限制的阅读、修改、分发文件是导致信息泄密的重要原因。

正是基于敏感信息资源泄密导致的严重危害性，越来越多的法律、法规对企业的信息安全行为作出了规定：要求保护公司机密信息，谨防不规范信息操作，防止未经授权造成的信息泄密和非法使用。

当前，信息泄密的主要途径有：

- 内部人员通过 U 盘或移动硬盘等移动存储设备从 PC 中将资料拷贝带走。
- 内部人员通过电子邮件将资料外发，导致泄密。
- 内部人员将资料打印后带出。
- 将办公用的便携式计算机直接带回家中窃取资料或将自己的便携式计算机带到公司，接入局域网，窃取资料。
- PC 易手后，硬盘上的资料没有及时删除，导致泄密。
- 随意将文件设成共享，导致非相关人员获取资料。
- 普通员工偷看公司机密文档。
- 存储介质丢失后，保存在存储介质上的资料被他人获取，导致信息泄密。

另外还有越来越多的因商业利益驱动的黑客窃密，使企业核心业务资源和商业机密被截获和侦听，给企业造成巨大损失，影响核心竞争力。

因此，防止信息泄密以及防止非授权的信息访问已被提上企业信息安全建设的重要日程。

1.2 产品简介

介绍 DSM 的主要特点。

DSM (Document Security Management) 文档安全管理软件是华为技术有限公司推出的针对机密文档，防止信息泄密的一款成熟产品。通过对企业的重要文档进行加密和实时权限控制，可为企业提供安全授权下的机密信息共享，使信息所有者能够定义信息的访问者、访问方式和时间等，并记录文档操作日志。有效防止因不受权限限制的阅读、修改、分发文件导致的信息泄密。

DSM 的主要功能包括：

- 文档权限管理
 - 只读
 - 修改
 - 完全控制
 - 打印
 - 复制
 - 分发
 - 离线
- 离线权限产指 DSM 客户端在不连接 DSM 服务器的情况下使用安全文档，主要用于终端用户出差后无法连接服务器的场景。
- 打开次数控制
 - 打印次数控制
 - 文档权限有效期控制
 - 安全文档还原

- 水印控制
- 防截屏控制
- 客户端设置文档权限
- Web 界面设置文档权限
- 客户端申请权限
- Web 界面查询和审批权限请求
- 邮件通知请求人和审批人
- 组策略和权限模板

组策略是若干用户与若干权限的集合。使用组策略来给一组用户或者部门进行集中授权，实现权限的统一管理。权限模板是由用户在 DSM 客户端创建，包含若干条用户信息和权限信息，仅供用户在本地计算机设置安全文档的访问权限时反复使用。权限模板提高了客户端授权的易用性，加快了个人用户的授权速度。
- 跨系统授权

DSM 支持分布式部署。在分布式部署下某地区的用户可以将文档的权限授予其他地区的用户或者部门。跨系统授权通过满足不同地区之间的文档授权需求，实现了不同地区之间的机密信息共享。
- 用户漫游

DSM 支持分布式部署。在分布式部署下用户可以接入非本地服务器进行打开文档和制作文档等操作。用户漫游适用于用户在归属地以外的地区办公，并且目的地区已经部署了 DSM 服务器的场合。
- 支持多种编辑器的控制

表1-1 DSM 支持的文件类型和编辑器

编辑器	扩展名	权限
包括简体中文版和英文版 (32-bit 版本和 64-bit 版本) : <ul style="list-style-type: none"> • Microsoft Office Word 2003 • Microsoft Office Excel 2003 • Microsoft Office PowerPoint 2003 	<ul style="list-style-type: none"> • .doc • .xls • .ppt 	<ul style="list-style-type: none"> • 只读 • 修改 • 复制 • 打印 • 分发 • 离线 • 完全控制
包括简体中文版和英文版 (32-bit 版本和 64-bit 版本) : <ul style="list-style-type: none"> • Microsoft Office Word 2007 • Microsoft Office Excel 2007 • Microsoft Office 	<ul style="list-style-type: none"> • .docx • .xlsx • .pptx 	

编辑器	扩展名	权限
PowerPoint 2007		
包括简体中文版和英文版 (32-bit 版本和 64-bit 版本) : <ul style="list-style-type: none"> • Microsoft Office Word 2010 • Microsoft Office Excel 2010 • Microsoft Office PowerPoint 2010 		
包括简体中文版和英文版: <ul style="list-style-type: none"> • Microsoft Windows XP (仅 32-bit 版本) 的记事本 • Microsoft Windows 7 (仅 32-bit 版本) 的记事本 	.txt	
<ul style="list-style-type: none"> • UltraEdit 17 简体中文版和英文版 (仅 32-bit 版本) 		
包括简体中文版和英文版 (32-bit 版本和 64-bit 版本) : <ul style="list-style-type: none"> • Adobe Reader 7.0 • Adobe Reader 8.0 • Adobe Reader 9.0 	.pdf	<ul style="list-style-type: none"> • 只读 • 复制 • 打印 • 分发 • 离线 • 完全控制

- 对外 API 接口支持
DSM 提供 API (Application Programming Interface) 应用编程接口, 第三方应用系统可以很容易的通过提供的 API 接口实现安全文档的制作、访问权限的修改、还原安全文档、申请安全文档权限以及修改安全文档所属的部门。
- 日志审计和自动转储
提供详细的文档日志和操作日志, 便于有效跟踪和审计用户的行为。
提供工具实现对文档日志和操作日志进行定期转储。
- 用户管理
支持同步 Microsoft AD 域控制器和 eDirectory 认证服务器的部门和账号信息。

1.3 产品特性

介绍 DSM 的主要特性。

DSM 充分考虑了大中型企业网络的应用特点，包含如下特性：

- **高安全性**
强大的动态加解密技术，分散管理文件、集中管理加密授权信息，实现密钥、权限与内容分离，为企业提供更高的安全性。
- **高可靠性**
DSM 支持冗余备份方式进行部署，保证单个服务器在意外情况下无法提供服务时其他服务器还可以继续提供服务。DSM 客户端会自动选择可用的 DSM 服务器获取服务。使用 Microsoft SQL Server 2005 的镜像技术进行数据存储,实现数据库的完全热备。
- **高性能**
DSM 使用负载均衡和本地缓存，大大提高了单位时间内可以处理的业务数。一个管理节点最多可支持 20000 个用户，每分钟最多可以处理 2000 个用户的请求。
- **灵活、方便的组网方案**
DSM 支持单套系统集中式组网，也支持多套系统进行分布式组网，联合工作。适用于各种大中型和小型公司。
- **可扩展性**
DSM 提供对外接口给第三方应用系统调用，实现文档的安全管理和授权。提供了统一的文档安全管理平台，具有良好的可扩展性。
- **标准性**
DSM 的设计开发完全遵从国际相关行业标准和软件工程管理规范，并完全采用通用化和模块化设计。

2 体系结构

关于本章

介绍 DSM 的系统组成以及各组成部分的配置要求。

2.1 系统组成

DSM 系统由 DSM 管理中心（可选）、DSM 服务器、数据库服务器、DSM 客户端、用户系统（可选）和 FTP（File Transfer Protocol）服务器（可选）组成。

2.2 配置要求

介绍了 DSM 的软、硬件配置要求。

2.1 系统组成

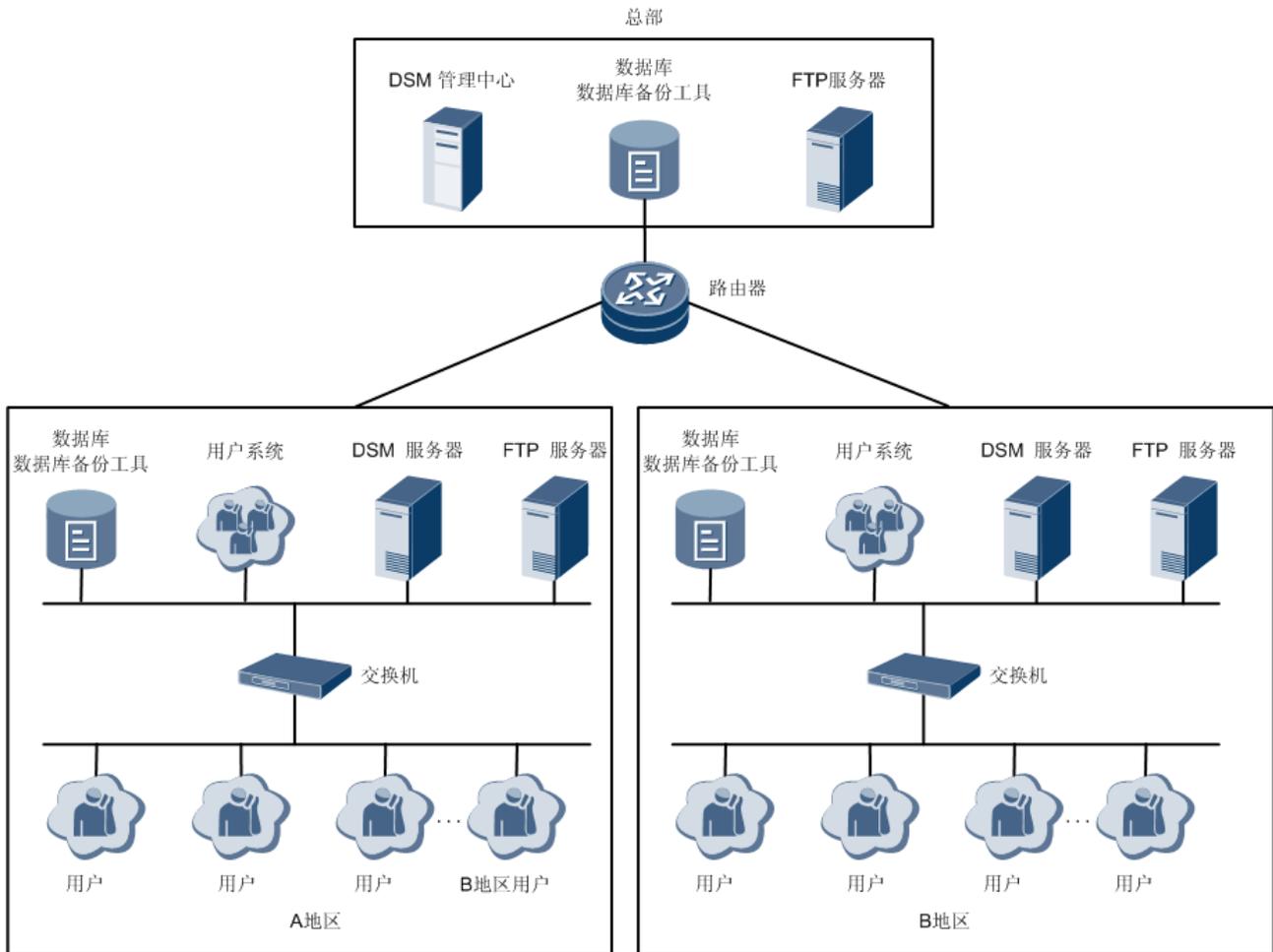
DSM 系统由 DSM 管理中心（可选）、DSM 服务器、数据库服务器、DSM 客户端、用户系统（可选）和 FTP（File Transfer Protocol）服务器（可选）组成。

2.1.1 组成图

介绍了 DSM 的系统组成图。

DSM 的系统组成图如图 2-1 所示。

图2-1 DSM 的系统组成图



DSM 各个子系统的功能如下：

- DSM 管理中心为可选安装组件，只有使用分布式组网时才需要安装。DSM 管理中心运行于 Microsoft Windows Server 2003，其作用有：
 - 向各个地区的文档安全管理服务器下发全局组策略和 License，为 DSM 服务器指派文档管理员。
 - 定期从各地区的 DSM 服务器收集部门信息和账号信息，然后将所有的部门信息和账号信息下发至各个地区的 DSM 服务器，以便完成跨地区授权功能。
 - 在所有部门信息和账号信息中查询指定部门、账号和文档管理员。
- DSM 服务器为必须安装的组件，其主要功能是向 DSM 客户端提供文档安全管理服务。

一个地区的文档安全服务通常由若干台（最多 4 台）DSM 服务器共同提供。在正常情况下，管理员配置该地区每台 DSM 服务器的权重，以便每台 DSM 服务器以负载分担的方式工作。当其中一台 DSM 服务器出现故障时，DSM 客户端将会尝试连接该地区的其他 DSM 服务器，确保访问安全文档业务不会被中断。

DSM 服务器采用 Microsoft Windows Server 2003 操作系统作为自身的运行平台，其主要功能有响应用户身份认证请求和访问安全文档的请求、管理安全文档及其访问权限、支持安全文档的跨区域授权、提供友好的 Web 界面。

- 数据库服务器

DSM 服务器采用 Microsoft SQL Server 2005 数据库或 Oracle 数据库作为自身的数据存储系统。

与 DSM 服务器相同，数据库服务器采用 Microsoft Windows Server 2003 操作系统作为自身的运行平台，其主要功能有存储本地用户信息、从用户系统同步复制的用户信息（可选）、本地部门信息、从用户系统同步复制的部门信息（可选）、安全文档的相关操作日志、安全文档的访问权限。

如果数据库服务器采用 Microsoft SQL Server 2005，则必须安装和配置数据库备份工具每天以完全备份的方式备份数据库，并且需要配备一台硬件服务器安装 FTP 服务，由数据库备份工具自动将数据库备份文件上传至 FTP 服务器保存，以便在数据库发生故障时恢复数据。

- DSM 客户端

DSM 客户端用于协助用户进行身份认证、制作安全文档、打开安全文档、查看安全文档的访问权限、调整安全文档的访问权限、还原安全文档，防止安全文档在使用过程中泄密。

需要访问安全文档的用户必须安装 DSM 客户端。DSM 客户端能够在如下操作系统运行：

- Microsoft Windows XP SP2 简体中文版和英文版
- Microsoft Windows XP SP3 简体中文版和英文版
- Microsoft Windows Vista 简体中文版和英文版

- 用户系统

存储企业或公司的用户信息，协助 DSM 服务器完成用户身份认证，以检查访问安全文档的用户是否合法。

DSM 服务器能够与已经部署好的用户系统联动，故管理员无须为 DSM 服务器单独部署用户系统。

目前 DSM 服务器只支持：

- Microsoft AD (Active Directory) 域控制器。
- LDAP 认证服务器，目前只支持 Novell eDirectory 认证服务器（简称 eDirectory 认证服务器）。

- FTP 服务器

FTP 服务器为可选安装组件。利用网络中的 FTP 服务器，向用户提供 DSM 客户端的下载和升级服务。另外，如果数据库服务器采用 Microsoft SQL Server 2005，FTP 服务器用来存储由数据库备份工具生成的数据库备份文件，以便在数据库发生故障时恢复数据。

2.1.2 DSM 管理中心

DSM 管理中心只在分布式部署的情况下才需要，其职责是管理 DSM 服务器，在各 DSM 服务器之间同步数据、下发组策略、为 DSM 服务器指定文档管理员。此外，还可以进行 License 管理。

DSM 管理中心的主要功能包括：

- 同步部门和账号
支持配置同步部门和账号的周期、立即同步部门和账号以及查看同步部门和账号的结果。经过同步部门和账号，各个地区的 DSM 服务器能从 DSM 管理中心同步复制整个企业所有地区的部门和账号信息，方便在跨系统授权访问时进行身份认证和权限校验。
- 全局组策略的管理
支持添加、查询、修改、删除和同步全局组策略。全局组策略是由系统管理员在 DSM 管理中心创建，在系统管理员执行同步组策略之后，在 DSM 管理中心管辖范围内的所有用户允许使用全局组策略。
- 管理节点管理
 - 支持代理配置
如果 DSM 管理中心与 DSM 服务器必须通过代理服务器才能互相通信，则系统管理员必须在 DSM 管理中心配置代理服务器的连接参数。
 - 支持增加、修改管理节点
管理节点由某地区的若干台 DSM 服务器组成。一个管理节点最多能包含 4 台 DSM 服务器。创建管理节点的目的在于 DSM 管理中心能够定期从各管理节点将各个地区的部门、账号信息同步复制到 DSM 管理中心，然后将所有的部门、账号信息下发给各个管理节点，以便完成跨系统授权访问安全文档。
 - 支持下发服务器
下发服务器是指 DSM 管理中心将所有的节点信息下发至各个地区的 DSM 服务器，以便各地了解其他地区 DSM 服务器的地址。
 - 支持查询下发结果
查询下发结果，以便系统管理员了解 DSM 管理中心所有的管理节点信息是否已经成功下发至所管辖的管理节点。
 - 支持对 DSM 服务器的监控
DSM 管理中心对管辖范围内的所有 DSM 服务器的运行状态进行监控。如果 DSM 服务器与 DSM 管理中心断开连接，系统会发送邮件告警及时通知告警邮件接收人。
 - 支持告警集中管理
DSM 管理中心定期收集管辖范围内的所有 DSM 服务器产生的告警信息，并发送邮件告警给 DSM 服务器和 DSM 管理中心的告警邮件接收人，便于实时查看异常告警信息，及时处理，从而确保系统稳定、可靠运行。
- 日志审计
 - 日志包括系统操作日志和文档日志。
 - 支持对所有日志的查询以及操作日志的下载功能。
 - 支持对 DSM 管理中心管辖范围内的所有 DSM 服务器的文档日志进行审计。
 - 支持对 DSM 管理中心管辖范围内的所有 DSM 服务器的安全文档进行查询。
- 部门管理
 - 支持查看所有部门和成员，以便系统管理员了解每个管理节点的部门信息、账号信息和文档管理员信息。

- 支持查询部门和成员。
- 支持添加、查询和删除所有地区的文档管理员。执行对文档管理员的操作后，无需同步，立即生效。
- 支持限制系统管理员和日志管理员从 Web 登录访问 DSM 管理中心的 IP 地址。
- License 管理
支持申请、上传、分配、立即下发和查询管理节点的 License。在无有效 License 的情况下，DSM 不支持终端用户连接 DSM 服务器进行身份认证。如果系统管理员需要增加用户的最大连接数，则需要申请 License。

2.1.3 DSM 服务器

DSM 服务器是 DSM 的核心组件。

DSM 服务器的主要功能包括：

- 部门管理
 - 部门结构支持多级方式，以树状结构进行管理。
 - 支持同步 Microsoft AD 域控制器和 eDirectory 认证服务器的部门和账号信息。
 - 支持添加、修改、查询、删除本地部门和用户。
 - 支持添加、查询和删除文档管理员。
 - 支持限制系统管理员、日志管理员和普通用户从 Web 登录的 IP 地址。
- 部门文档管理
部门文档是指隶属于某部门及其子部门的用户制作的所有安全文档的集合。为了方便部门的安全文档管理，每个部门将会指定若干个文档管理员。由文档管理员来统一管理本部门及其子部门的所有安全文档。一个部门最多可添加 40 个文档管理员。
 - 文档管理员通过给用户、部门和所有人授权，应用组策略以及删除权限来调整部门文档的访问权限。
 - 支持本部门文档管理员给其子部门添加、删除文档管理员。
- 文档权限管理
 - 支持只读、修改、完全控制的基本权限。
 - 支持打印、复制、分发、离线、打开次数控制、打印次数控制、文档权限有效期控制、安全文档还原、水印控制、防截屏控制的附加权限。
 - 支持通过客户端进行权限申请，并邮件通知权限审批人。
 - 支持审批权限请求，并邮件通知权限请求人。
 - 提供 Web 界面对安全文档的权限进行修改。
- 本地系统组策略和本地部门组策略管理
组策略是若干用户与若干权限的集合，根据组策略类型以及创建者的不同可供所有用户或局部地区的用户用来设置安全文档的权限。
DSM 服务器提供的是对本地系统组策略和本地部门组策略的管理。
 - 提供本地系统组策略或本地部门组策略来给一组用户或者部门进行集中授权，实现权限的统一管理。

- 支持系统管理员添加、查询、修改、删除本地系统组策略。
- 支持文档管理员添加、查询、修改、删除本部门及其子部门的本地部门组策略。
- 支持负载均衡

权重是指为 DSM 服务器分配一个系数，通过设置该系数的大小来调整 DSM 客户端连接该 DSM 服务器进行通信的概率。通过配置服务器及权重，可以避免因 DSM 客户端总是与固定的一台 DSM 服务器通信造成的负载不均衡的问题。

支持增加、修改、删除 DSM 服务器及权重。
- 日志审计
 - 日志包括系统管理日志和文档操作日志。
 - 支持日志的查询和下载功能。
- 定制版权信息
 - 支持定制 DSM 客户端的版权信息，系统管理员可以在 DSM 服务器上设置 DSM 客户端的登录图片、版权和登录标题。
 - 支持定制 DSM 服务器的版权信息，系统管理员可以在 DSM 服务器上设置 DSM 服务器的登录图片、首页图片、版权、登录标题、技术网站、和电子邮件。
- 客户端升级
 - 客户端自动升级

系统管理员可以配置 DSM 客户端自动升级的时间段，默认情况下，一天升级一次。
 - 客户端强制升级

支持配置允许接入的客户端的最低版本。如果客户端版本低于此版本，那么客户端进行任何业务操作时都会提示版本过低，需要手工升级到指定版本。
 - 客户端版本统计

系统管理员按照版本号、IP 地址、姓名、MAC 地址等来统计终端用户的数量，以此评估升级进展。
- License 管理

支持申请、上传 License。在无有效 License 的情况下，DSM 不支持用户连接 DSM 服务器进行身份认证。如果系统管理员需要增加用户的最大连接数，则需要申请新的 License。在 DSM 服务器不受 DSM 管理中心控制的情况下，支持通过 DSM 服务器进行 License 管理。

2.1.4 DSM 客户端

DSM 客户端主要负责文档权限的控制、制作安全文档、打开安全文档等。

安全文档是由 DSM 生成的电子文档，并且通过 DSM 来授权控制其他用户的访问权限。用户必须通过 DSM 服务器的身份认证和权限验证才允许打开安全文档。

DSM 客户端的主要功能包括：

- 制作安全文档

通过制作安全文档、设置安全文档的访问权限为普通文档提供保护功能。只有通过身份认证和权限校验的用户才允许打开安全文档，降低机密信息泄密的风险。

- 申请安全文档的访问权限
用户对安全文档不具备相应的访问权限时，能够通过 DSM 客户端向安全文档的作者、拥有完全控制权限的用户或文档管理员提出权限申请。
- 查看安全文档的访问权限
查看安全文档的访问权限，以便了解被授权用户对该安全文档具有哪些访问权限。
- 打开安全文档
只有拥有只读或以上权限的用户才允许打开安全文档。
- 修改安全文档的内容
只有拥有修改权限的用户（包括作者）才有权限修改安全文档的内容。修改并保存的安全文档依然处于受保护状态，在拥有访问权限的用户通过身份认证之后才能访问。在修改安全文档的内容之后，访问权限不会发生变化。
- 修改安全文档的访问权限
只有作者、文档管理员、拥有分发权限的用户、拥有完全控制权限的用户才能修改安全文档的访问权限。
- 应用组策略
在制作安全文档或修改安全文档的访问权限时，通过应用组策略以便快速设置用户或部门的访问权限。
- 还原安全文档
还原安全文档是指将“.dsm”格式的安全文档转换为原始格式的普通文档。只有作者和被授予完全控制权限的用户才能还原安全文档。在还原安全文档之后，访问普通文档不再受到权限限制。
- 离线访问安全文档
离线访问安全文档适用于在出差时用户无法连接 DSM 服务器，在文档管理员或文档作者批准的情况下依然能够访问安全文档的场景。
- 跨系统授权
跨系统授权是指在分布式部署情况下，A 地区的用户制作好安全文档后，给 B 地区的用户授予该安全文档的访问权限。而 B 地区的用户在获得安全文档后，能够依据授予的访问权限实现对安全文档的使用。
- 用户漫游
当离开归属地后，用户需要通过连接非归属地的 DSM 服务器进行身份认证，从而进行打开文档和制作文档等操作。用户漫游适用于在分布式部署情况下，用户在归属地以外的地区办公，并且目的地区已经部署了 DSM 服务器的场合。
- 客户端手动升级
当确定 DSM 服务器上已经存在新版本的客户端升级程序可用时，通过手动升级将当前版本的 DSM 客户端升级至新版本。

2.2 配置要求

介绍了 DSM 的软、硬件配置要求。

2.2.1 服务器配置要求

介绍了 DSM 管理中心、DSM 服务器和数据库服务器的配置要求。

DSM 管理中心、DSM 服务器、数据库服务器的软、硬件配置要求均相同，配置要求请参见表 2-1。

表2-1 软、硬件配置要求

配置项	配置要求
CPU	Xeon 四核 5405(2.0GHz 或以上) × 2
内存	4GB(1GB × 4)或以上
硬盘	146GB × 5
网卡	2 个或以上
电源	100V ~ 240V AC
操作系统	Microsoft Windows Server 2003 标准简体中文版或英文版，32 位，带 SP2 补丁。 推荐配置 Microsoft Windows Server 2008 R2 标准简体中文版或英文版，64 位。
数据库	Microsoft SQL Server 2005 标准简体中文版或英文版，32 位，带 SP2 补丁。 推荐配置 Microsoft SQL Server 2008 标准简体中文版或英文版，32 位。 Microsoft SQL Server 2008 标准简体中文版或英文版，64 位。
UI 管理界面	Microsoft Internet Explorer 6.0 或 Microsoft Internet Explorer 7.0

2.2.2 客户端配置要求

介绍了 DSM 客户端的配置要求。

DSM 客户端推荐的软、硬件配置要求请参见表 2-2。

表2-2 DSM 客户端软、硬件配置要求

配置项	建议配置
CPU	Intel Pentium 4 1.0GHz 或以上
内存	512MB 或以上
硬盘	10GB 或以上
软件预留安装空间	500MB 或以上
支持的操作系统（32位）	<ul style="list-style-type: none">• Microsoft Windows XP SP2 简体中文版或英文版• Microsoft Windows XP SP3 简体中文版或英文版• Microsoft Windows Vista 简体中文版或英文版• Microsoft Windows 7 简体中文版或英文版
支持的操作系统（64位）	<ul style="list-style-type: none">• Microsoft Windows XP SP2 简体中文版或英文版• Microsoft Windows XP SP3 简体中文版或英文版• Microsoft Windows 7 简体中文版或英文版

3 组网方案

关于本章

介绍 DSM 的组网方案，包括集中式组网和分布式组网。

3.1 集中式组网

在组织机构的总人数不超过 2 万人的情况下，只需部署一套 DSM，即一个管理节点。

3.2 分布式组网

在组织机构的总人数超过 2 万人且分布在若干个地区的情况下，建议采用分布式组网。

3.1 集中式组网

在组织机构的总人数不超过 2 万人的情况下，只需部署一套 DSM，即一个管理节点。

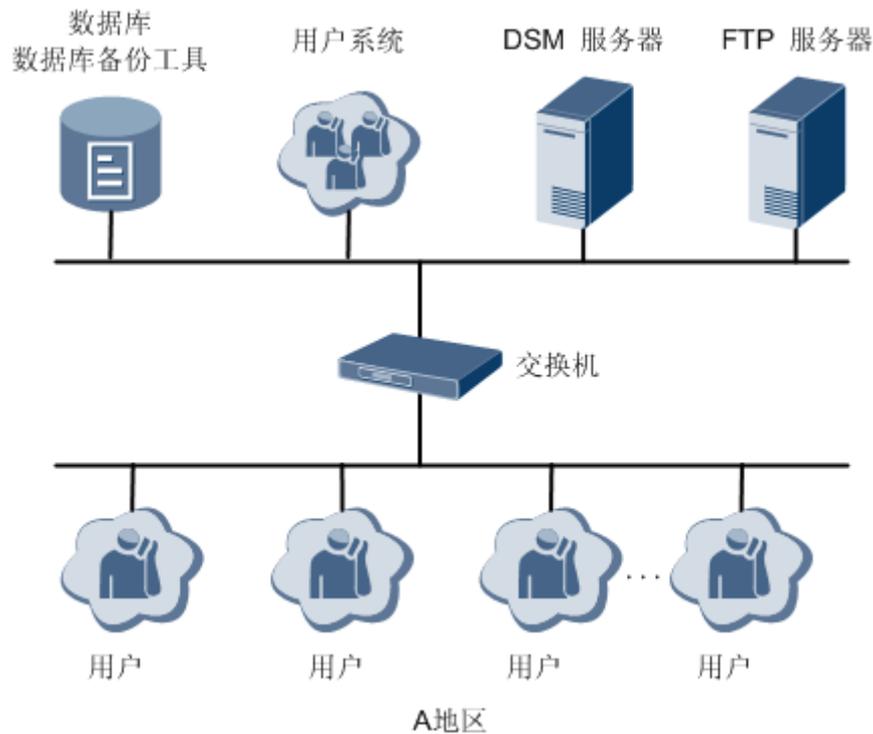
一个管理节点主要由 DSM 服务器、数据库服务器、DSM 客户端和 FTP 服务器组成。

集中式组网的硬件服务器规划如下：

- 如果不需要负载均衡功能，只需要部署 1 台安装有 DSM 服务器的硬件服务器。
- 如果需要负载均衡功能，需要部署 2 台或 2 台以上硬件服务器，每台硬件服务器均需要安装 DSM 服务器。
- 如果不需要数据库的热备份功能，只需要部署 1 台安装有 Microsoft SQL Server 2005、Microsoft SQL Server 2005 的 SP2 补丁和数据库备份工具的硬件服务器。
- 如果需要数据库的热备份功能，需要部署 3 台硬件服务器，每台硬件服务器均需安装 Microsoft SQL Server 2005 及 Microsoft SQL Server 2005 的 SP2 补丁。主数据库和镜像数据库需要安装数据库备份工具。
- FTP 服务器为数据库备份文件提供存在媒介。

DSM 的集中式组网如图 3-1 所示。

图3-1 DSM 的集中式组网方案



集中式组网规划请参见表 3-1。

表3-1 集中式组网规划

配置项	规划
PC 数量	1 ~ 20000。
License 数量	License 数量由 PC 数量决定，所有的 License 均由 DSM 服务器统一分配，具体的操作请参见“配置 License”。
部门与账号	规划 DSM 如何对用户进行身份认证： <ul style="list-style-type: none"> • 如果网络中已经安装了 Microsoft AD 域控制器，建议采用 DSM 与 Microsoft AD 域控制器联动的方式，将 Microsoft AD 域控制器现有的组织结构复制到 DSM 服务器，并使用 Microsoft AD 域账号对用户进行身份认证，具体的操作请参见“从 Microsoft AD 域控制器同步部门和账号”。 • 如果网络中已经安装了 eDirectory 认证服务器，建议采用 DSM 与 eDirectory 认证服务器联动的方式，将 eDirectory 认证服务器现有的组织结构复制到 DSM 服务器，并使用 eDirectory 账号对用户进行身份认证，具体的操作请参见“从 eDirectory 认证服务器同步部门和账号”。 • 如果网络中未安装 Microsoft AD 域控制器和 eDirectory

配置项	规划
	认证服务器，建议在 DSM 服务器上创建本地部门和本地账号，并使用本地账号对用户进行身份认证，具体的操作请参见“在不安装用户系统时规划部门和账号”。本地部门和本地账号存储在数据库中，不需要另外规划硬件服务器。
DSM 服务器	需要 1 台~4 台硬件服务器，保留 80 端口、443 端口、8015 端口和 8019 端口。C 盘安装 Microsoft Windows Server 2003 标准版，Microsoft Windows Server 2003 的 SP2 补丁和 DSM 服务器。 <ul style="list-style-type: none"> • 如果不需要负载均衡功能，需要部署 1 台硬件服务器安装 DSM 服务器。 • 如果需要负载均衡功能，需要部署 2 台~4 台硬件服务器，每台硬件服务器均需要安装 DSM 服务器。
数据库服务器	需要 1 台或 3 台硬件服务器，保留 1433 端口。C 盘安装 Microsoft Windows Server 2003 标准版，同时需要安装 Microsoft Windows Server 2003 的 SP2 补丁。D 盘预留 60GB 或以上的空闲空间，用于安装 Microsoft SQL Server 2005、Microsoft SQL Server 2005 的 SP2 补丁和数据库备份工具。 <ul style="list-style-type: none"> • 如果不需要数据库的热备份功能，需要部署 1 台硬件服务器安装 Microsoft SQL Server 2005、Microsoft SQL Server 2005 的 SP2 补丁和数据库备份工具。 • 如果需要数据库的热备份功能，需要部署 3 台硬件服务器，每台硬件服务器均需要安装 Microsoft SQL Server 2005、Microsoft SQL Server 2005 的 SP2 补丁，主数据库和镜像数据库需要安装数据库备份工具。
FTP 服务器	需要 1 台硬件服务器，用于存储数据库备份工具产生的数据库备份文件，以便在数据库出现故障时恢复数据库，减少因数据库故障或数据损坏造成的损失。
DSM 客户端	需要 1 台 PC，目标分区预留 100MB 或以上的空闲空间。只支持在下列操作系统安装 DSM 客户端： <ul style="list-style-type: none"> • Microsoft Windows XP SP2 简体中文版和英文版 • Microsoft Windows XP SP3 简体中文版和英文版 • Microsoft Windows Vista 简体中文版和英文版 • Microsoft Windows 7 简体中文版和英文版

3.2 分布式组网

在组织机构的总人数超过 2 万人且分布在若干个地区的情况下，建议采用分布式组网。

DSM 在分布式部署上主要分两级架构：

- DSM 管理中心
DSM 管理中心统一对下面的管理节点进行系统管理，指派各个管理节点的文档管理员等。
- 管理节点
一个管理节点主要由 DSM 服务器、数据库服务器、DSM 客户端、FTP 服务器组成，也就是一个集中式组网。

分级架构提供了用户扩展功能，支持用户权限的跨系统授权和漫游功能。

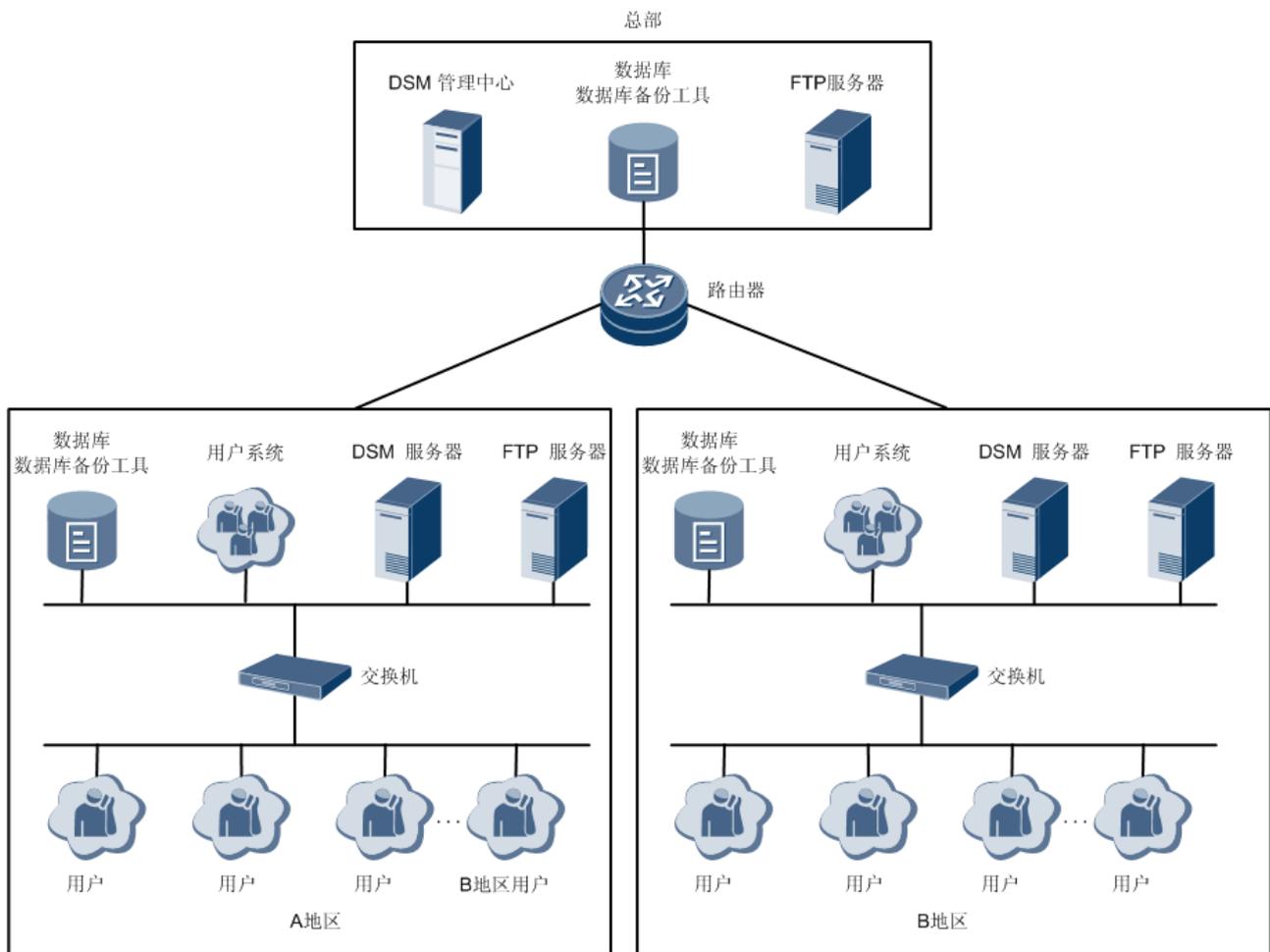
在分级部署中，通过配置 DSM 管理中心，系统管理员可以统一管理各个地区的 DSM 服务器。在各 DSM 服务器之间同步数据，实现跨系统授权，漫游登录，创建全局组策略，下发 DSM 服务器列表，为各个 DSM 服务器的部门指定文档管理员。

分布式组网的硬件服务器规划包括：

- DSM 服务器的硬件服务器规划请参见表 3-2。
- DSM 管理中心的硬件服务器规划如下：
 - 如果不需要数据库的热备份功能，需要部署 2 台硬件服务器。一台用于安装 DSM 管理中心，一台用于安装 Microsoft SQL Server 2005 及 Microsoft SQL Server 2005 的 SP2 补丁。
 - 如果需要数据库的热备份功能，需要部署 4 台硬件服务器，一台用于安装 DSM 管理中心，剩下三台用于安装 Microsoft SQL Server 2005 及 Microsoft SQL Server 2005 的 SP2 补丁。
 - FTP 服务器，需要部署 1 台硬件服务器。主要用于安装 FTP 软件，存储由数据库备份工具生成的数据库备份。

DSM 的分布式组网如图 3-2 所示。

图3-2 DSM 的分布式组网方案



每个地区节点的规划请参见表 3-2。

表3-2 每个地区节点的规划

配置项	规划
PC 数量	1 ~ 20000。
License 数量	License 数量由 PC 数量决定。 <ul style="list-style-type: none"> • 如果 License 由 DSM 管理中心统一分配，则每个地区的系统管理员无须进行任何 License 配置。在 DSM 管理中心统一分配 License 的具体操作请参见“软件许可管理”。 • 如果 DSM 管理中心对 License 不作统一分配，则每个地区的系统管理员需要根据 PC 数量规划 License 数量，具体的操作请参见“配置 License”。
部门与账号	规划 DSM 如何对用户进行身份认证：

配置项	规划
	<ul style="list-style-type: none"> • 如果网络中已经安装了 Microsoft AD 域控制器，建议采用 DSM 与 Microsoft AD 域控制器联动的方式，将 Microsoft AD 域控制器现有的组织结构复制到 DSM 服务器，并使用 Microsoft AD 域账号对用户进行身份认证，具体的操作请参见“从 Microsoft AD 域控制器同步部门和账号”。 • 如果网络中已经安装了 eDirectory 认证服务器，建议采用 DSM 与 eDirectory 认证服务器联动的方式，将 eDirectory 认证服务器现有的组织结构复制到 DSM 服务器，并使用 eDirectory 账号对用户进行身份认证，具体的操作请参见“从 eDirectory 认证服务器同步部门和账号”。 • 如果网络中未安装 Microsoft AD 域控制器和 eDirectory 认证服务器，建议在 DSM 服务器上创建本地部门和本地账号，并使用本地账号对用户进行身份认证，具体的操作请参见“在不安装用户系统时规划部门和账号”。本地部门和本地账号存储在数据库中，不需要另外规划硬件服务器。
DSM 服务器	<p>需要 1 台~4 台硬件服务器，保留 80 端口、443 端口、8015 端口和 8019 端口。C 盘安装 Microsoft Windows Server 2003 标准版，Microsoft Windows Server 2003 的 SP2 补丁和 DSM 服务器。</p> <ul style="list-style-type: none"> • 如果不需要负载均衡功能，需要部署 1 台硬件服务器安装 DSM 服务器。 • 如果需要负载均衡功能，需要部署 2 台~4 台硬件服务器，每台硬件服务器均需要安装 DSM 服务器。
数据库服务器	<p>需要 1 台或 3 台硬件服务器，保留 1433 端口。C 盘安装 Microsoft Windows Server 2003 标准版，同时需要安装 Microsoft Windows Server 2003 的 SP2 补丁。D 盘预留 60GB 或以上的空闲空间，用于安装 Microsoft SQL Server 2005、Microsoft SQL Server 2005 的 SP2 补丁和数据库备份工具。</p> <ul style="list-style-type: none"> • 如果不需要数据库的热备份功能，需要部署 1 台硬件服务器安装 Microsoft SQL Server 2005、Microsoft SQL Server 2005 的 SP2 补丁和数据库备份工具。 • 如果需要数据库的热备份功能，需要部署 3 台硬件服务器，每台硬件服务器均需要安装 Microsoft SQL Server 2005 及 Microsoft SQL Server 2005 的 SP2 补丁，主数据库和镜像数据库需要安装数据库备份工具。
FTP 服务器	<p>需要 1 台硬件服务器，用于存储数据库备份工具产生的数据库备份文件，以便在数据库出现故障时恢复数据库，减少因数据库故障或数据损坏造成的损失。</p>

配置项	规划
DSM 客户端	需要 1 台 PC，目标分区预留 100MB 或以上的空闲空间。 只支持在下列操作系统安装 DSM 客户端： <ul style="list-style-type: none"> • Microsoft Windows XP SP2 简体中文版和英文版 • Microsoft Windows XP SP3 简体中文版和英文版 • Microsoft Windows Vista 简体中文版和英文版 • Microsoft Windows 7 简体中文版和英文版

管理中心节点的规划请参见表 3-3。

表3-3 管理中心节点的规划

配置项	规划
DSM 管理中心	需要 1 台硬件服务器，80 端口、443 端口、8015 端口和 8019 端口。C 盘安装 Microsoft Windows Server 2003 标准版，Microsoft Windows Server 2003 的 SP2 补丁和 DSM 管理中心。
数据库服务器	需要 1 台或 3 台硬件服务器，保留 1433 端口。C 盘安装 Microsoft Windows Server 2003 标准版，同时需要安装 Microsoft Windows Server 2003 的 SP2 补丁。D 盘预留 60GB 或以上的空闲空间，用于安装 Microsoft SQL Server 2005、Microsoft SQL Server 2005 的 SP2 补丁和数据库备份工具。 <ul style="list-style-type: none"> • 如果不需要数据库的热备份功能，需要部署 1 台硬件服务器安装 Microsoft SQL Server 2005、Microsoft SQL Server 2005 的 SP2 补丁和数据库备份工具。 • 如果需要数据库的热备份功能，需要部署 3 台硬件服务器，每台硬件服务器均需要安装 Microsoft SQL Server 2005 及 Microsoft SQL Server 2005 的 SP2 补丁，主数据库和镜像数据库需要安装数据库备份工具。
FTP 服务器	需要 1 台硬件服务器，用于存储数据库备份工具产生的数据库备份文件，以便在数据库出现故障时恢复数据库，减少因数据库故障或数据损坏造成的损失。

4 功能特性

关于本章

介绍 DSM 的功能特性。

4.1 文档权限管理

DSM 的文档权限包括只读、修改、完全控制的基本权限以及打印、复制、分发、离线的附加权限等。

4.2 组策略和权限模板

介绍 DSM 的组策略和权限模板。

4.3 跨系统授权

介绍在分布式部署情况下，DSM 的跨系统授权功能的应用。

4.4 用户漫游

介绍在分布式部署情况下，DSM 漫游功能的应用。

4.5 文件类型和编辑器

介绍 DSM 支持的文件类型和编辑器。

4.6 对外 API 接口支持

介绍 DSM 提供的对外 API 接口支持。

4.7 日志管理

介绍 DSM 的日志管理的具体功能。

4.8 用户和部门管理

介绍 DSM 的用户和部门管理的具体功能。

4.9 服务器管理

DSM 管理中心只在分布式部署的情况下才需要，其职责是对管理节点进行管理。

4.1 文档权限管理

DSM 的文档权限包括只读、修改、完全控制的基本权限以及打印、复制、分发、离线的附加权限等。

文档权限管理的具体功能包括：

- 只读权限
拥有只读权限的用户或部门，仅允许阅读安全文档，无法对安全文档进行修改、复制等操作。
- 修改权限
拥有修改权限的用户或部门，允许修改安全文档。在该安全文档内可以进行任何修改（包括在安全文档内部的内容复制和粘贴，从其他文档复制内容粘贴到该安全文档），但不能另存为其他文档，也无法将安全文档的内容复制并粘贴到其他文档。
- 完全控制
拥有完全控制权限的用户或部门，对该安全文档的操作不受限制，允许完全控制安全文档。
- 打印权限
拥有打印权限的用户或部门，允许打印安全文档。除具有完全控制权限的用户或部门外，其他的用户仅允许进行物理打印，不允许进行虚拟打印。
- 复制权限
拥有复制权限的用户或部门，允许将该安全文档中的内容复制到其他文档。
- 分发权限
拥有分发权限的用户或部门，允许在不超过自身权限的条件下调整现有安全文档的权限设置，或者将已经获得的除分发权限之外的权限再次授予其他用户或部门。
- 离线权限
拥有离线权限的用户或部门，允许用户不连接 DSM 服务器，即在离线状态下仍能够使用安全文档。每次以离线方式访问安全文档时，必须输入有权限以离线方式访问该安全文档的账号和密码，以便验证该用户是否合法。
- 打开次数控制
对具有只读或只读以上权限的用户设置最多能打开安全文档的次数。
- 打印次数控制
对具有打印权限的用户设置最多能打印安全文档的次数。
- 文档权限有效期控制
可以给某个用户指定访问安全文档的有效期，有效期包括开始时间和截止时间，超出有效期后用户不再具备对该安全文档的访问权限。
- 支持安全文档还原
只有作者和具有完全控制权限的用户可以在 DSM 客户端把安全文档还原成普通文档。
- 水印控制

打印安全文档时设置水印，以便有效的追踪文档泄密的渠道。DSM 服务器提供对水印的格式和内容的设置。

- 防截屏控制
只要打开安全文档，就不能通过各种截屏和录像工具对 PC 屏幕内容进行录制，降低安全文档泄密的风险。
- 通过客户端设置安全文档权限
支持应用组策略、权限模板或自行选择用户、部门及权限的方式设置安全文档的权限。通过客户端来设置安全文档权限的速度快、方便，建议用户优先选用该方法来设置安全文档权限。
- 通过 Web 界面设置安全文档权限
作者、文档管理员、具有分发权限和完全控制权限的用户可以对安全文档进行添加、删除组策略，添加、修改、删除用户或部门权限的操作。作者的权限不能被修改和删除。
- 通过客户端申请安全文档权限
用户对安全文档不具备相应的访问权限时，能够通过 DSM 客户端向安全文档的作者、拥有完全控制权限的用户或文档管理员提出权限申请。
- 通过 Web 界面查询、审批权限请求
用户通过客户端申请安全文档的访问权限后，请求人能够登录 DSM 服务器查询权限申请记录，审批人能够登录 DSM 服务器查询权限审批记录并进行审批处理。
- 支持邮件通知请求人和审批人
如果申请人和审批人在系统中登记了邮箱地址，则系统会在提交权限申请和审批处理后分别给审批人和申请人发送邮件通知。
- 普通用户管理自己制作的安全文档
普通用户登录 DSM 服务器 Web 界面查询自己制作的安全文档、查看自己制作的安全文档的操作日志以及调整由自己创建的安全文档的访问权限。查询条件支持文档名、摘要、创建时间范围、更新时间范围，并支持模糊查询。查询结果可以按查询条件进行排序，支持分页显示。
- 普通用户管理可授权的安全文档
可授权文档是指用户拥有该安全文档的分发权限或完全控制权限，允许该用户为其他用户授予该安全文档除分发权限外所有自身的权限。
普通用户登录 DSM 服务器 Web 界面查询可授权的安全文档、查看可授权的安全文档的操作日志以及调整可授权的安全文档的访问权限。查询条件支持文档名、摘要、作者账号、作者姓名、所属部门、创建时间范围、更新时间范围、文档权限，并支持模糊查询。查询结果可以按查询条件进行排序，支持分页显示。
- 文档管理员管理自己有权限的部门文档
文档管理员登录 DSM 服务器 Web 界面查询可以管理的部门文档、查看部门文档的操作日志以及调整部门文档的访问权限。查询条件支持文档名、摘要、作者账号、作者姓名、所属部门、创建时间范围、更新时间范围，并支持模糊查询。查询结果可以按查询条件进行排序，支持分页显示。

4.2 组策略和权限模板

介绍 DSM 的组策略和权限模板。

组策略是由 DSM 服务器的系统管理员、DSM 服务器的文档管理员或 DSM 管理中心的系统管理员创建，包含若干条用户信息和权限信息。在制作安全文档或修改安全文档的访问权限时，用户只需引用组策略，即可快速为组策略中包含的所有用户设置指定的访问权限。

而权限模板是由用户在 DSM 客户端创建，包含若干条用户信息和权限信息，仅供用户在本地计算机设置安全文档的访问权限时反复使用。

组策略和权限模板的主要功能包括：

- 支持添加、修改、删除全局组策略
DSM 管理中心的系统管理员登录 DSM 管理中心添加、修改、删除全局组策略。全局组策略由策略名、策略类型、创建时间、策略描述和组策略列表组成，最多可支持 300 条组策略。全局组策略对 DSM 管理中心管辖范围内各个地区的所有 DSM 服务器均可见。
全局组策略可以定期下发到每个 DSM 服务器，也可以手动下发。
- 支持添加、修改、删除本地系统组策略
DSM 服务器的系统管理员登录 DSM 服务器添加、修改、删除本地系统组策略。本地系统组策略由策略名、策略类型、创建时间、策略描述和组策略列表组成，最多可支持 300 条组策略。本地系统组策略只对本地区 DSM 服务器可见，对其他地区的 DSM 服务器不可见。
- 支持添加、修改、删除本地部门组策略
DSM 服务器的文档管理员登录 DSM 服务器添加、修改、删除本部门或其子部门的本地部门组策略。只有连接本地区 DSM 服务器的该部门或其子部门的用户才允许使用。
- 支持使用权限模板
DSM 客户端在授权时，可以把当前的权限保存到一个文件作为模板，方便以后应用。权限模板包括权限列表，但是不包含授权人和作者权限信息。
DSM 客户端在授权时，可以选择一个权限模板文件把权限应用到当前文档。用户在客户端应用模板前，可以查看模板的详细信息，用于确认应用的模板是正确的。

4.3 跨系统授权

介绍在分布式部署情况下，DSM 的跨系统授权功能的应用。

在 DSM 中支持文档跨系统授权，为企业提供跨系统的文档信息保护。

文档的跨系统授权是指 A 地区的用户制作好安全文档后，给 B 地区的用户授予该安全文档的访问权限。而 B 地区的用户在获得安全文档后，能够依据授予的访问权限实现对安全文档的使用。

跨系统授权需要 DSM 管理中心能够定期从所有的 DSM 服务器中将各个地区的部门、账号信息同步复制到 DSM 管理中心，然后再将所有的部门、账号信息下发给各个地区的 DSM 服务器，以便完成跨系统授权。

4.4 用户漫游

介绍在分布式部署情况下，DSM 漫游功能的应用。

当离开归属地后，用户需要通过连接非归属地的 DSM 服务器进行身份认证，从而进行打开文档和制作文档等操作。

当 B 地区的用户到 A 地区出差时，B 地区的用户必须通过漫游登录的方式连接 A 地区的 DSM 服务器进行身份认证，从而实现与本地登录完全相同的后续操作（如制作安全文档、获取和修改安全文档的权限）。

用户漫游适用于在分布式部署情况下，用户在归属地以外的地区办公，并且非归属地已经部署了 DSM 服务器的场合。

4.5 文件类型和编辑器

介绍 DSM 支持的文件类型和编辑器。

DSM 支持的文件类型和编辑器包括：

表4-1 DSM 支持的文件类型和编辑器

编辑器	扩展名	权限
包括简体中文版和英文版（32-bit 版本和 64-bit 版本）： <ul style="list-style-type: none">• Microsoft Office Word 2003• Microsoft Office Excel 2003• Microsoft Office PowerPoint 2003	<ul style="list-style-type: none">• .doc• .xls• .ppt	<ul style="list-style-type: none">• 只读• 修改• 复制• 打印• 分发• 离线• 完全控制
包括简体中文版和英文版（32-bit 版本和 64-bit 版本）： <ul style="list-style-type: none">• Microsoft Office Word 2007• Microsoft Office Excel 2007• Microsoft Office PowerPoint 2007	<ul style="list-style-type: none">• .docx• .xlsx• .pptx	

编辑器	扩展名	权限
包括简体中文版和英文版 (32-bit 版本和 64-bit 版本) : <ul style="list-style-type: none"> • Microsoft Office Word 2010 • Microsoft Office Excel 2010 • Microsoft Office PowerPoint 2010 		
包括简体中文版和英文版: <ul style="list-style-type: none"> • Microsoft Windows XP (仅 32-bit 版本) 的记事本 • Microsoft Windows 7 (仅 32-bit 版本) 的记事本 	.txt	
<ul style="list-style-type: none"> • UltraEdit 17 简体中文版和英文版 (仅 32-bit 版本) 		
包括简体中文版和英文版 (32-bit 版本和 64-bit 版本) : <ul style="list-style-type: none"> • Adobe Reader 7.0 • Adobe Reader 8.0 • Adobe Reader 9.0 	.pdf	<ul style="list-style-type: none"> • 只读 • 复制 • 打印 • 分发 • 离线 • 完全控制

4.6 对外 API 接口支持

介绍 DSM 提供的对外 API 接口支持。

DSM 提供的对外 API 接口支持是由 DSM 客户端提供的，具体包括：

- 提供对外 API 接口给外部应用系统制作安全文档
- 提供对外 API 接口给外部应用系统修改安全文档权限
- 提供对外 API 接口给外部应用系统还原安全文档
- 提供对外 API 接口给外部应用系统申请安全文档权限
- 提供对外 API 接口给外部应用系统修改安全文档所属部门

4.7 日志管理

介绍 DSM 的日志管理的具体功能。

日志管理的主要功能包括：

- 支持查询、下载操作日志
日志管理员可以查询和下载系统管理员、文档管理员和普通用户的操作日志。
- 提供详细的操作日志
操作日志包括用户在 DSM 服务器上的操作日志以及在 DSM 管理中心上的操作日志。
- 支持查询、下载文档日志
日志管理员可以查询和下载文档日志，并且作者和文档管理员分别可以查看自己有权限的文档日志。
- 提供详细的文档日志
文档日志监控用户对安全文档进行的所有操作。
- 提供离线操作时的离线日志
DSM 客户端在进行离线操作时，暂时把日志信息保存到本地，连接到 DSM 服务器后把日志上报到服务器用于审计。
- 支持对 DSM 管理中心管辖范围内的所有 DSM 服务器的日志审计
DSM 管理中心的日志管理员可以审计 DSM 管理中心管辖范围内的所有 DSM 服务器的文档日志。
- 提供日志自动转储功能
提供工具实现对文档日志和操作日志进行定期转存。

4.8 用户和部门管理

介绍 DSM 的用户和部门管理的具体功能。

用户和部门管理的主要功能包括：

- 支持本地用户管理
系统管理员在 DSM 服务器上可以查询、创建、修改、删除本地用户。
- 支持本地部门管理
系统管理员在 DSM 服务器上可以查询、创建、修改、删除本地部门。
- 支持本地用户口令修改
本地用户可以登录 DSM 服务器 Web 界面修改自己的口令，并且系统管理员可以强制初始化用户的口令。
- 支持系统管理员口令强度
系统管理员修改后的口令长度需要大于或等于 8 个字符，小于或等于 20 个字符，并且必须同时包含大写字母、小写字母、数字和特殊字符。
- 同步 Microsoft AD 域控制器上的部门和账号信息

系统管理员登录 DSM 服务器 Web 界面同步 Microsoft AD 域控制器上的账号和部门信息。支持同步多个 Microsoft AD 域控制器上的部门和账号信息，并按顺序对部门和账号进行排序。同步账号的内容包括账号、姓名、用户邮箱。

- 同步 eDirectory 认证服务器上的部门和账号信息

系统管理员登录 DSM 服务器 Web 界面同步 eDirectory 认证服务器上的账号和部门信息，支持同步多个 eDirectory 认证服务器上的部门和账号信息，并按顺序对部门和账号进行排序。同步账号的内容包括账号、姓名、用户邮箱。

- 支持查询用户和部门

系统管理员登录 DSM 服务器后，能够根据用户或者部门的相关信息查询用户和部门。

- 支持添加、查询、删除文档管理员

系统管理员可以添加、查询、删除文档管理员，每个文档管理员都跟部门相关联。本部门的文档管理员可以给其子部门添加、删除文档管理员。

- 支持限制 Web 登录的地址

支持限制系统管理员和日志管理员从 Web 登录访问 DSM 服务器或 DSM 管理中心的 IP 地址，同时也支持限制普通用户从 Web 登录访问 DSM 服务器的 IP 地址，从而保证了系统的安全性。

4.9 服务器管理

DSM 管理中心只在分布式部署的情况下才需要，其职责是对管理节点进行管理。

服务器管理的主要功能包括：

- 支持对 DSM 服务器的统一配置和管理

管理节点由某地区的若干台 DSM 服务器组成。一个管理节点最多能包含 4 台 DSM 服务器。系统管理员可以在 DSM 管理中心添加管理节点，一台 DSM 管理中心最多支持 50 套管理节点。DSM 管理中心能够在管辖范围内的管理节点之间同步数据、下发组策略、以及为 DSM 服务器指定文档管理员。

- 支持对 DSM 服务器的监控

DSM 管理中心对管辖范围内的所有 DSM 服务器的运行状态进行监控。如果 DSM 服务器与 DSM 管理中心断开连接，系统会发送邮件告警及时通知系统管理员。

- 支持告警集中管理

DSM 管理中心定期收集管辖范围内的所有 DSM 服务器产生的告警信息，并发送邮件告警给系统管理员，便于系统管理员实时查看异常告警信息，及时处理，从而确保系统稳定、可靠运行。