针对中小企业以目录服务为基础的统一资源管理存储解决方案

深圳市安普储域科技有限公司

2014 年 12 月

目　录

前 言 2
1　统一资源管理的必要性 3
2　统一资源管理所用目录服务技术背景 3
2.1 LDAP（Lightweight Directory Access Protocol）轻量目录存取协议 4
2.2 微软活动目录（AD） 5
3　APT 的 UQ 系列统一存储，为 SMB 提供基于目录服务统一认证的所有数据服务 6
4　以目录服务为基础的统一认证：UnifiedAUTH 9
4.1 UnifiedAUTH 的优势 10
4.2 在 UQ316 系列统一存储系统上配置目录服务 11
4.3 附加服务：为使用 UQ316 统一存储的用户规划和设计 AD 域 14

前 言

企业的统一资源管理是负责保存、管理该企业及所属各子公司所有的人员、组织、工作组、角色、应用系统和域名规则等信息资源，为企业门户系统及各应用系统提供资源管理、身份认证、资源互联互访、访问鉴权、域名管理和数据整合等服务的。

统一资源管理通常以目录服务技术为基础，本文将介绍 APT 的统一存储产品通过集成目录服务帮助中小企业实现统一资源管理。

1 统一资源管理的必要性

企业在信息化的实践过程中会逐步建立邮件、OA、以文件共享为基础的协同办公、ERP等应用为核心的 IT 架构，是企业成功、高效运营的重要保障。但是各应用系统面向企业的不同管理方向，各有其对应的用户群体、技术架构、权限体系，限制了系统之间的信息共享和信息交换，形成企业的信息孤岛。同时，每一个员工（应用系统的用户）在企业中拥有不同的角色（职能），需要操作不同的系统，难以对其需要和拥有的信息和操作进行综合处理，限制了企业信息化系统效率的发挥。实施企业门户系统是解决上述问题的好方案。其中统一资源管理系统是企业门户系统的一个重要组成部分。

统一资源管理将分散的资源进行统一、集中的管理，应用统一身份管理实现企业门户用户身份的统一认证，改变原有各业务系统中的分散式身份认证及鉴权管理，实现对用户的集中认证和鉴权管理，简化用户访问内部各系统的过程，使得用户只需要通过一次身份认证过程就可以访问具有相应权限的所有资源。

2 统一资源管理所用目录服务技术背景

目录是一种专门的数据库，它服务于各种应用程序，包括 LDAP（轻量级目录访问协议）目录和基于 X.500 的目录。目录包含条目的说明性信息，以描述一个企业内用户为例，其目录包括姓名、电话号码、电邮地址等，当然还有账号和密码。目录数据库是以树状的层次结构来描述数据信息的。这种模型与众多行业应用的业务组织结构完全一致，如政府部门、行政单位和企业的机构设置、人员和资源的组织方式。由于在现实世界中存在大量的层次结构，采用目录数据库技术的信息管理系统就能够轻易地做到与实际的业务模式相匹配。显然，目录服务非常适于基于目录和层次结构的信息管理。

目录服务实际上就是一种信息查询服务，它依赖于树状结构的目录数据库来提供信息查询。目录服务可广泛应用于网络本身的资源管理、网络信息的组织和查询。对于企业来说，目录服务器主要用来实现整个网络系统各种资源的管理，作为网络的一种基础架构，支持网络结构化、安全认证、资源集中管理和资源共享等功能。目录服务可以：

- 按照管理员的定义强制实施安全性以保持信息的安全，以防入侵者的攻击；

- 在一个网络的多台计算机间分配目录，提供更高的性能；
- 复制目录，以使更多的用户可以使用目录，同时有效地防止失败的发生；
- 将目录划分为多个数据源（存储区），以便存储大量对象。

2.1 LDAP（Lightweight Directory Access Protocol）轻量目录存取协议

LDAP（Lightweight Directory Access Protocol）轻量目录存取协议是一个快速增长的对通用目录信息进行存取访问的技术。LDAP 已经被大多数面向网络的中间层所应用和实现。作为一个开放，独立于任何厂商的标准，LDAP 为目前分布式系统和服务中所要求的中央化信息存贮和管理提供了一个可扩展的结构。LDAP 已经成为目录信息的标准方式，这非常象 DNS 一样用于在大多数 Internet/Intranet 系统中对 IP 地址的查询，LDAP 现在为大多数的网络操作系统，组件系统和应用所支持。

LDAP 是以树状的层次结构来存储数据。很多系统的配置系统和组织结构方式都可以用树型结构来模型化。LDAP 服务器可以用“推”或“拉”的方法复制部分或全部数据，允许根据需要使用 ACI 控制对数据读和写的权限。LDAP 技术的应用是实现网络服务、目录存储和用户信息以及网络资源信息统一管理的技术基础。

LDAP 是在 TCP/IP 之上运行的轻型目录访问协议，它定义以下内容：

(1)目录信息基于条目。条目是一个属性集合，每个属性具有唯一的辨识名(DN)。DN 用来无二义性的引用条目。每个条目的属性都有类型和值。类型常为助记字符串，值的语法依赖于属性类型。

(2)目录条目按层次树型结构排列，这种结构正好反应了现实中事物的组织结构。按域名来构造目录树的方法越来越流行，因为它允许使用域名系统来定位目录服务。

(3)对目录中的条目可以进行添加、删除、修改等操作，甚至可以对条目名进行修改，但用得最多的是搜索操作。通过在搜索过滤器中指定相应的条件，可以只对某个子树中的条目进行搜索，从而大大缩小了搜索范围。

(4)一些条目加以保护，允许有授权的人访问。一些条目可以使用用户验证机制或访问控制机制来保证目录中信息的安全性。

2.2 微软活动目录（AD）

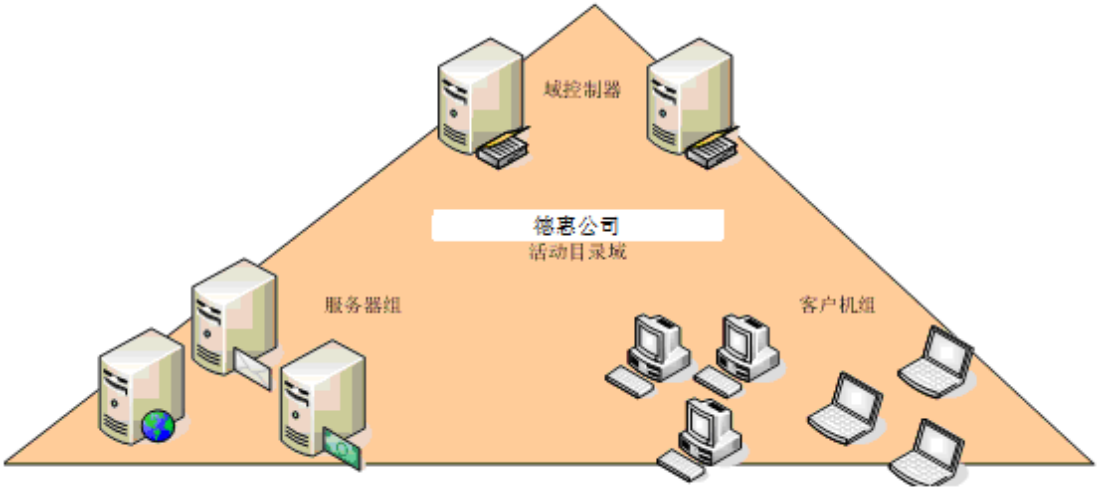
活动目录（AD）是微软基于 LDAP 提供给服务器平台的目录服务。域（domain）是逻辑上的概念，通常是一个安全边界，主要是提供对资源的集中控制和简化管理。

活动目录（AD）是 Windows Server 2008/2012 网络体系结构中一个基本且不可分割的部分，它为网络的用户、管理员和应用程序提供了一套分布式网络环境设计的目录服务。活动目录（AD）使得组织机构可以有效地对有关网络资源和用户的信息进行共享和管理。另外，目录服务在网络安全方面也扮演着中心授权机构的角色，从而使操作系统可以轻松地验证用户身份并控制其对网络资源的访问。应用微软活动目录（AD）的好处如下表所示：

优势	描述
提升用户效率	● 活动目录中的用户可以登录到任何一台属于活动目录中的计算机 ● 方便快速的安装网络打印机 ● 快速查找电话号码与员工信息
增强安全性	● 限制用户使用计算机 ● 限制用户登录的时间 ● 要求用户使用复杂的密码 ● 限制 USB 接口和打印机的使用等
减轻 IT 管理负担与成本	● 软件自动安装或按需安装 ● 软件自动更新 ● 软件自动卸载 ● 用户端桌面管理 ● 管理授权，可对组织单元实现委派控制

与应用集成	● 与众多应用集成，优化应用管理

在一个 AD 单域，企业用户的所有计算机（服务器和客户机）全部加入到域，用户实现单一登录和管理员通过域组策略实现安全及桌面管理。AD 架构拓扑如下。

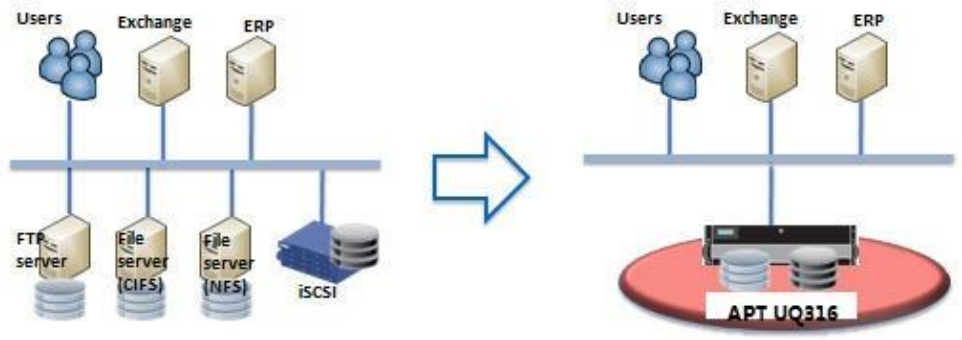


3 APT 的 UQ 系列统一存储，为 SMB 提供基于目录服务统一认证的所有数据服务

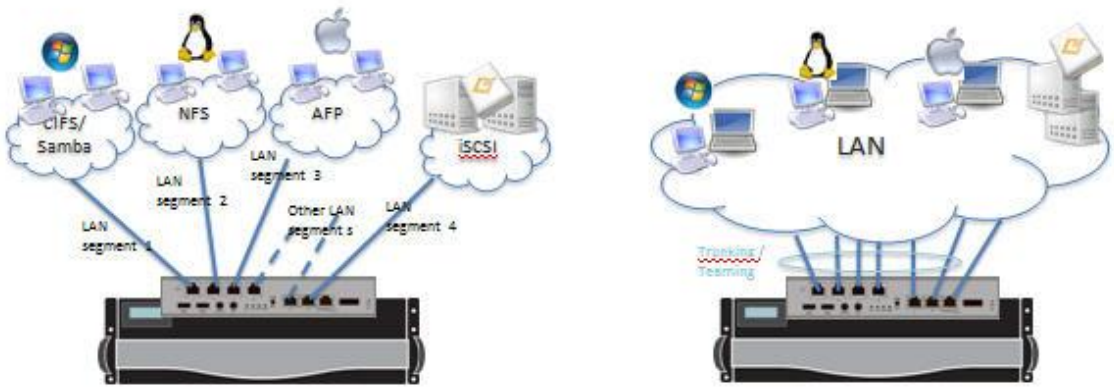
相对于结构化数据（即行数据，存储在数据库里，可以用二维表结构来逻辑表达实现的数据）而言，不方便用数据库二维逻辑表来表现的数据即称为非结构化数据，包括所有格式的办公文档、文本、图片、XML、HTML、各类报表、图像和音频/视频信息等。据 IDC 的一项调查报告中指出：企业中 80%的数据都是非结构化数据，这些数据每年都按指数增长 60%以上。1%-5%的企业数据库数据是结构化的数据。NAS 存储技术的存储设备在管理非结构化数据安装部署和管理是相当容易的，而 SAN 存储技术的设备更适用于管理结构化数据。APT 的 UQ316 系列统一存储是在同一时间同时支持文件级和数据块级访问的 RAID 存储系统，同时支持 NAS 和 IP SAN 存储技术，并且由一个统一界面管理文件和块数据、提

升存储利用率，其优势是集中，存储管理简单、高效。

中小企业用户所需要的多种数据服务：文件共享（CIFS、NFS、AFP）、FTP 服务器以及 iSCSI 存储，全都由 APT 的 UQ316 系列统一存储在一个“机箱”中提供和满足了，而且用户访问在 UQ316 系列统一存储中的共享数据无需附加任何硬件。



APT 的 UQ316 系列统一存储允许用户进行灵活的组网连接，具体如下：



Service	Management port	LAN1 ~ LANn
HTTP (Download QCentral page)	Yes	No
CIFS	Yes	Yes
NFS	Yes	Yes
AFP	Yes	Yes
WebDAV	No	Yes
iSCSI	Yes	Yes
Link aggregation	No	Yes

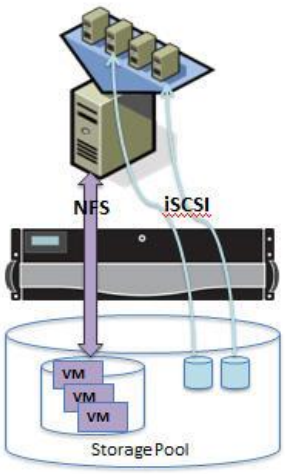
APT 在 UQ316 系列统一存储上创新和专利的统一认证（UnifiedAUTH）简化了企业内部 IT 系统的账户管理，所有的数据服务（CIFS、NFS、APF、FTP、iSCSI 和 WebDAV 等）都采用同一组账户和密码进行认证和登录；用户不用担心忘记密码。

下面列出了 APT 的 UQ316 系列统一存储系统产品的一些应用场景：

- **服务器虚拟化**

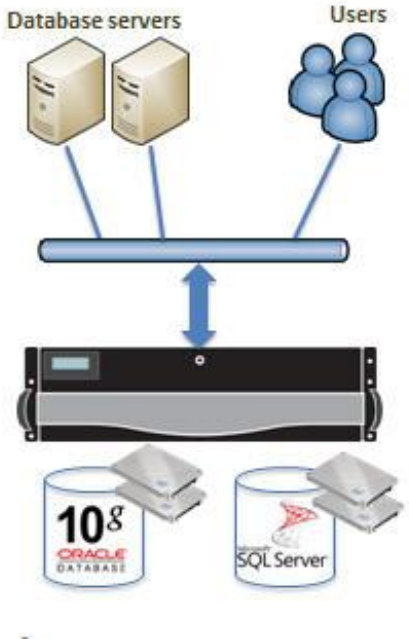
用户在部署他们的服务器虚拟化环境时都会因性能方面的要求而对基于数据块的裸设备映射（RDM）提出要求，UQ316 系列统一存储为用户如何存储他们的虚机（VM）提供了选择，而无需像之前那样分别购买 SAN 和 NAS 存储设备。

- UQ316 系列统一存储系统为服务器虚拟化的系统管理程序虚机监视器提供数据存储以保持和更新虚机（VM）的影像，并由 NFS 连接提供该数据存储的 I/O 通道。
- UQ316 系列统一存储系统为虚机（VM）上的应用需求提供 iSCSI 数据块级存储；
- 利用 UQ316 系列统一存储系统上重复数据删除和自动精简配置功能来实现更高的存储效率。



➢ **在线数据库应用**

- UQ316 系列统一存储系统为微软 Sharepoint、Oracle 数据库和微软 SQL 数据库等应用提供数据块级存储；
- 由 UQ316 系列统一存储系统上的 ZFS 文件系统提供数据保护功能；
- 使用 SSD 盘作为 ZFS 文件系统的 L2ARC Cache 来达成更好的随机读 IOPS 性能；
- 提供更佳的存储效率。



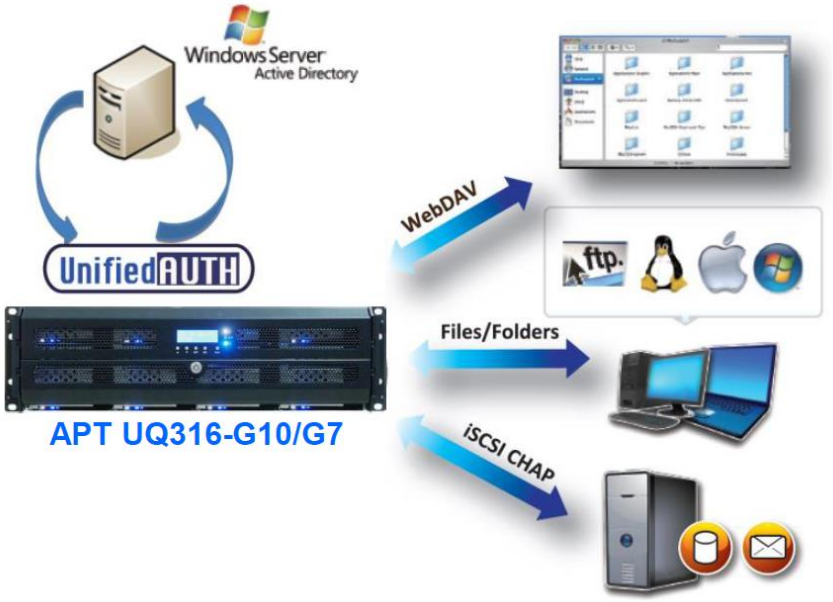
4 以目录服务为基础的统一认证：UnifiedAUTH

UnifiedAUTH 是统一认证的缩写。在一个企业的网络环境中，数据的安全是绝对必须和关键的要素，数据安全的基本实现方法是对共享的文件夹进行访问控制，即进行授权和认证。认证就需要用户提供账号和密码。

在许多案例中，不同的文件共享服务由不同的服务器和各自的账户、密码来提供，用户需要为 CIFS、FTP、AFP 和 iSCSI 等不同的数据存储服务熟记不同的账户和密码。因此 APT UQ316 系列统一存储系统的目标就是集中不同数据服务的硬件需求、减少存储管理的复杂

性、增加存储的效率，在 UQ316 系列统一存储系统上提供的 UnifiedAUTH 准许用户使用同样的账户和密码访问所有的数据服务：CIFS、NFS、AFP、FTP、iSCSI 和 WebDAV。

UnifiedAUTH 类似于单点登录的概念，但这不是它的工作方式。当用户第一次为各种数据服务建立数据连接时，用户仍然需要输入账号和密码。UnifiedAUTH 更像欧洲的申根签证（Schengen Visa）的概念，拥有了合法的申根签证（Schengen Visa），你就可以在欧洲各国旅行。



4.1 UnifiedAUTH 的优势

UnifiedAUTH 可为企业客户的 IT 管理者带来真正的方便。以一个有 200 名员工的中等规模企业为例，如果 NAS 存储系统不支持目录服务与所有数据服务的集成，一个单独的 FTP 账户和一个单独的 iSCSI CHAP 身份验证协议账户及目录服务账户将带来 3 组不同的账户和管理，这意味着企业的 IT 管理者需要维护 200 x 3 = 600 个记录，随之而来的还会有更多种账户管理的要求，这对企业 IT 管理来说简直是个噩梦。对于 NAS 存储的用户来说，每人都需要为不同的数据服务记住 3 个不同的密码；如果存储需求增长，第二或第三台 NAS 增加到企业 IT 环境中，则更多的密码需要记住、更多的账户需要维护。UnifiedAUTH 解决了上述问题并给用户带来以下好处：

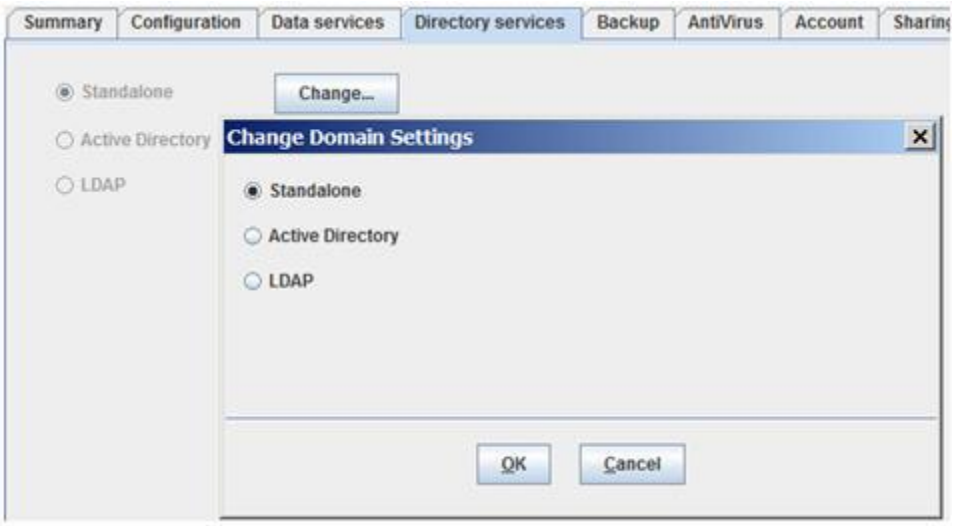
- 一组账户和密码使用户可方便地使用统一存储上所有的数据服务；

- 简化存储的管理。

4.2 在 UQ316 系列统一存储系统上配置目录服务

在 APT 的存储管理软件 QCentral 的界面中选择“目录服务”标签，APT 的 UQ316 系列统一存储系统提供以下三种目录服务：

- 独立的目录服务（缺省设置）
- 微软活动目录（AD）
- LDAP



缺省设置是独立的目录服务，在该模式下在 UQ316 统一存储上只有本地用户和组被建立，在同一时间只能有一种数据服务被激活；这样做是为减少混乱、增加效率。

1、 独立的目录服务（缺省设置）

当用户的 IT 网络环境中没有目录服务时，用户可在 APT 的 UQ316 统一存储上简单地建

立用户账户和组账户，并用它们来访问存储上提供的所有数据服务；缺省的用户是：admin 和 user，缺省的组是：administrator_group 和 user_group。

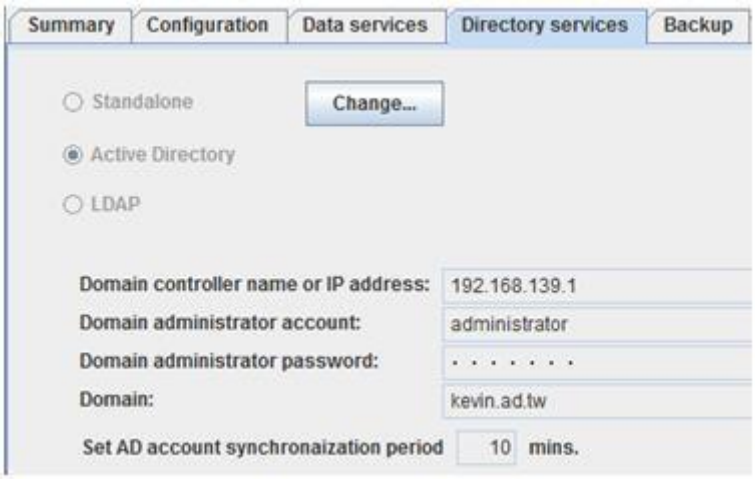
因为UnifiedAUTH集成了iSCSI CHAP账户验证，因此密码有12-16个字符的长度限制，否则会被三种目录服务拒绝。

在用户建立本地账户前，需确认具有主目录功能的存储池已被激活，否则用户不能建立本地账户，所有功能是灰色无法点击的。

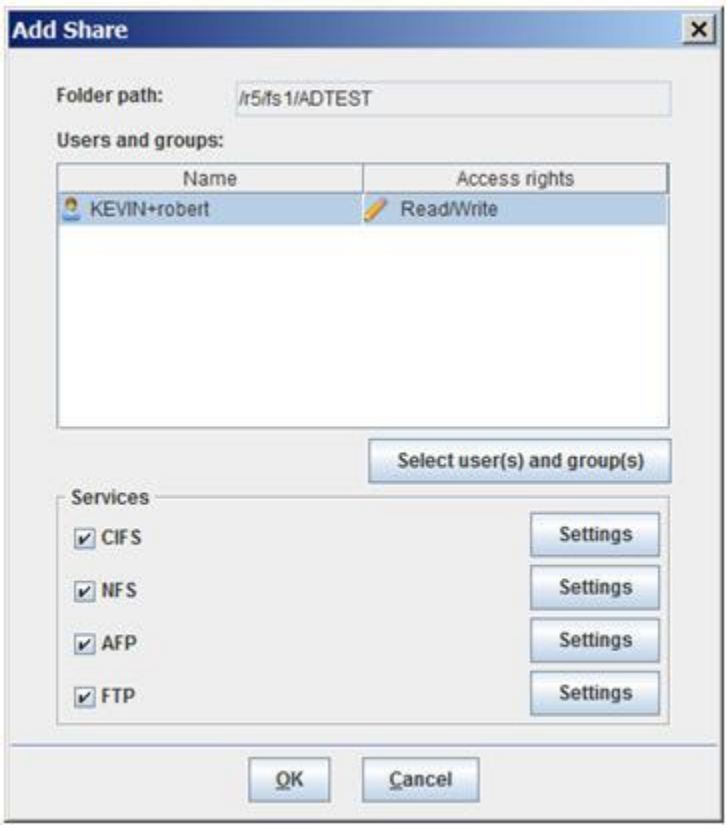
2、 微软活动目录（AD）

APT的UQ316统一存储支持Windows Server 2003/2008/2012 R2的AD，所有AD和LDAP账户都被视为域帐户，用户不能更改域帐户的属性，只能查看；编辑域帐户需到AD服务器或LDAP服务器上进行，最大的域帐户数是65536。

下图是UQ316统一存储加入AD域(kevin)后的截屏：

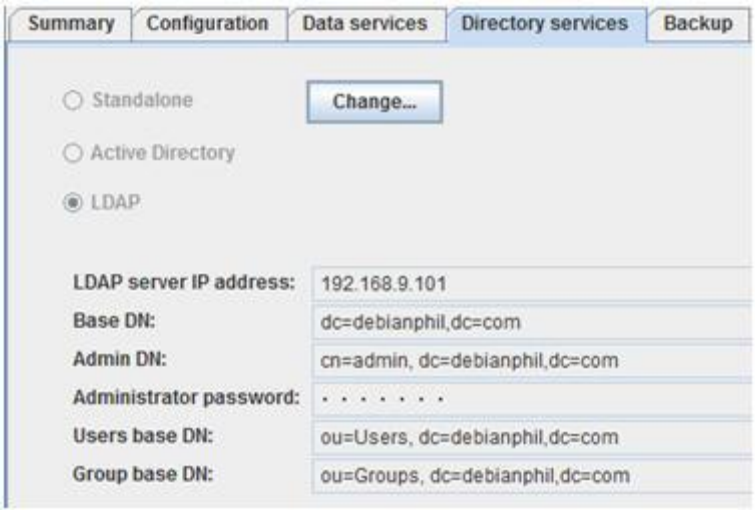


UQ316统一存储加入AD域(kevin)后，可为每个域帐户增加、设置允许访问的数据服务类型（见下图，为域帐户 kevin\robert 设置可访问的数据服务）。



3、 LDAP

APT 的 UQ316 统一存储支持 LDAP 版本 3，LDAP 也是一种流行的目录服务，LDAP 账户也被视为域帐户，用户不能更改域帐户的属性，只能查看；最大的域帐户数是 65536。下图是 UQ316 统一存储登录到 LDAP 服务器后的截屏：



4.3 附加服务：为使用 UQ316 统一存储的用户规划和设计 AD 域

如果计划使用 UQ316 统一存储的用户希望同时部署微软活动目录（AD），希望所有的计算机分阶段加入到域，通过活动目录加强计算机安全和桌面管理，并为进一步部署 Exchange 等打下坚实的基础架构，请联系我们：support@apt-storage.cn。