

به نام خدا

آفرینش و انسانیت در آن



مؤلفین:

مصطفی امینی (پژوهشگر و مدرس دانشگاه)

مکارشناس ارشد مهندسی نرم افزار

مریم رضائی (پژوهشگر حوزه فناوری اطلاعات)

مکارشناس مهندسی نرم افزار

سرشناسه	: امینی، مصطفی، ۱۳۶۳ -
عنوان و نام پدیدآور	: آفرسکو و امنیت در آن / مولفین مصطفی امینی، مریم رضائی.
مشخصات نشر	: تهران: آتی‌نگر، ۱۳۹۲.
مشخصات ظاهری	: ۲۲۴ص: مصور، جدول، نمودار.
شابک	: 978-600-6004-75-4
وضعیت فهرست نویسی	: فیپا
یادداشت	: واژه‌نامه.
موضوع	: رسانه‌های رقمی -- مدیریت
موضوع	: سیستم‌های چندرسانه‌ای -- مدیریت
موضوع	: ترافیک متن‌باز
شناسه افزوده	: رضایی، مریم، ۱۳۶۶ -
رده بندی کنگره	: Q۷۶/۵۷۵/الف ۱۷ ۱۳۹۲
رده بندی دیویی	: ۰۰۴/۷



انتشارات آتی‌نگر

عنوان: آفرسکو و امنیت در آن

مؤلفین: مهندس مصطفی امینی، مهندس مریم رضائی

ناشر: آتی‌نگر

تیراژ: ۱۰۰۰

طراحی جلد: محمد نورمحمدی (نورسا سامانه)

حروف چینی و صفحه‌آرایی: همتا بیداریان

چاپ اول: ۱۳۹۲

قیمت: ۲۱۷,۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۶۰۰۴-۷۵-۴

تلفن مرکز پخش: ۰۹۳۵۷۱۷۱۷۱۳ - ۶۶۵۶۵۳۳۶-۸

آدرس: تهران - خیابان جمالزاده جنوبی - روبه‌روی کوچه رشتچی - پلاک ۱۴۴ - واحد ۲

www.ati-negar.com

(هرگونه کپی و نسخه‌برداری از مطالب این کتاب ممنوع می‌باشد).

فهرست مطالب

پیشگفتار

۱۳

مقدمه

۱۵

فصل اول: سیستم‌های مدیریت محتوای سازمانی آفرسکو

۱۷

- ۱-۱ سیستم مدیریت محتوای سازمانی ۱۸
- ۱-۲ مؤلفه‌های یک سیستم مدیریت محتوای سازمان ۱۹
- ۱-۲-۱ مدیریت محتوای سازمانی از دیدگاه فناوری ۲۰
- ۱-۲-۲ فناوری‌های تشکیل دهنده ECM ۲۱
- ۱-۳ آفرسکو؛ تاریخچه و معرفی ۲۲
- ۱-۳-۱ معرفی سیستم مدیریت محتوای آفرسکو ۲۳
- ۱-۳-۲ اجزا و قابلیت‌های سیستم مدیریت محتوای سازمانی آفرسکو ۲۷
- ۱-۳-۳ یکپارچه‌سازی در آفرسکو ۲۸
- ۱-۳-۴ زبان آفرسکو ۲۹
- ۱-۴ نصب برنامه آفرسکو ۳۰
- ۱-۴-۱ نصب به صورت پیش فرض ۳۱
- ۱-۴-۲ نصب به صورت پیشرفته ۳۹

۵۴	۲-۱ مدل عضوگیری و امنیت در آلفرسکو
۵۴	۲-۲ فضاها
۵۵	۲-۲-۱ کاربران و گروه‌ها
۵۷	۲-۳ مدیریت کاربران سیستم
۵۷	۲-۳-۱ ایجاد کاربران جدید
۶۲	۲-۳-۲ ویرایش جزئیات کاربری
۶۳	۲-۳-۳ شامل کردن اطلاعات پروفایل مدیر و تغییر رمز عبور
۶۴	۲-۳-۴ حذف یک کاربر از سیستم
۶۴	۲-۳-۵ جست‌وجو برای کاربران موجود در Alfresco Exploer
۶۴	۲-۴ مدیریت گروه‌های کاربری
۶۵	۲-۴-۱ ساخت گروه‌ها و زیر گروه‌ها
۶۷	۲-۴-۲ اضافه کردن کاربران به گروه‌ها
۶۸	۲-۴-۳ حذف کاربران از یک گروه
۶۹	۲-۴-۴ جست‌وجو در آلفرسکو

۷۸	۳-۱ افزودن یک کاربر جدید
۸۱	۳-۲ ادمین کاربری
۸۲	۳-۳ گروه‌ها و Records Management
۸۳	۳-۴ جست‌وجو نام دیگر کاربران
۸۳	۳-۵ جست‌وجوی گروه
۸۴	۳-۶ افزودن یک گروه جدید
۸۵	۳-۷ حذف یک گروه
۸۵	۳-۸ ویرایش گروه
۸۵	۳-۹ افزودن اعضا به گروه

۸۷	۳-۱۰ سایت
۸۷	۳-۱۰-۱ دسترسی اعضا به اسناد مدیریت سایت
۸۷	۳-۱۰-۲ اشتراک در سایت مدیریت رکوردها
۸۸	۳-۱۱ ایجاد سایت
۹۱	۳-۱۲ درخواست دسترسی به سایت محدود شده Records Management
۹۳	۳-۱۳ دسترسی شخصی به سایت Records Management

فصل چهارم: مدیریت نقش‌ها و مجوزها

۹۵	۴-۱ بررسی امنیت در آفرسکو
۹۶	۴-۲ مدل امنیت آفرسکو
۹۷	۴-۳ مجوزها و قانون‌ها
۹۷	۴-۳-۱ نقش‌های پیش‌فرض
۹۹	۴-۴ قوانین
۹۹	۴-۴-۱ انواع راه‌اندازی
۱۰۰	۴-۵ دعوت کاربران یا گروه‌ها به فضای خود
۱۰۵	۴-۶ تعریف و امن‌سازی فضای شخصی
۱۰۵	۴-۷ دعوت کردن کاربران برای دسترسی به محتوا
۱۰۸	۴-۸ تمدید مجوزهای امنیتی و نقش‌ها
۱۰۹	۴-۸-۱ مجوزهای پیش‌فرض
۱۰۹	۴-۹ ایجاد یک نقش سفارشی
۱۱۰	۴-۱۰ نقش کاربر در یک فضا
۱۱۱	۴-۱۱ نقش‌های کاربری برای محتوا
۱۱۲	۴-۱۲ ایجاد امنیت در پوشه‌ها
۱۱۵	۴-۱۳ ایجاد امنیت در فایل‌ها

فصل پنجم: مدیریت نقش‌ها و مجوزها در Alfresco Share

۱۱۸	۵-۱ نقش‌ها و مجوزها
۱۱۸	۵-۲ دسترسی به کنترل‌های اعمال شده به طرح فایل
۱۱۹	۵-۳ مشاهده و ویرایش نقش‌های Records Management
۱۱۹	۵-۴ مرور مجوزهای نقش
۱۲۴	۵-۵ ویرایش مجوزهای نقش
۱۲۵	۵-۶ ایجاد یک نقش جدید
۱۲۵	۵-۷ حذف یک نقش
۱۲۵	۵-۸ خواندن و فایل کردن مجوزها
۱۲۶	۵-۹ گزارش حقوق کاربری (The User Rights Report)
۱۲۷	۵-۹-۱ چگونگی کارکرد
۱۲۷	۵-۹-۲ مدیریت کنسول کاربران
۱۲۸	۵-۱۰ کاربران در مخزن
۱۲۹	۵-۱۱ کاربران به عنوان User:user
۱۳۰	۵-۱۲ کاربران به عنوان Cm:person
۱۳۳	۵-۱۳ دسترسی به نقش از طریق وب اسکرپت
۱۳۴	۵-۱۴ مجوزها

فصل ششم: احراز هویت در آلفرسکو

۱۳۹	۶-۱ احراز هویت
۱۳۹	۶-۲ اختیارات
۱۴۰	۶-۳ زیرسیستم احراز هویت آلفرسکو
۱۴۰	۶-۳-۱ انواع زیر سیستم احراز هویت
۱۴۰	۶-۴ زنجیره احراز هویت
۱۴۱	۶-۵ تأیید نمونه‌های پیکربندی
۱۴۲	۶-۶ خصوصی سازی AlfrescoNtlm

۱۴۲	۶-۶-۱ ترکیب زنجیره احراز هویت
۱۴۳	۶-۶-۲ پیکربندی Instance
۱۴۴	۶-۷ پیکربندی LDAP برای متمرکز نمودن مدیریت شناسه‌ها
۱۴۸	۶-۸ هماهنگ‌سازی LDAP
۱۴۸	۶-۹ زنجیره مبتنی

فصل هفتم: راه‌حل‌های متقارن برای احراز هویت

۱۵۳

۱۵۴	۷-۱ احراز هویت و مفاهیم متقارن
۱۵۴	۷-۱-۱ احراز هویت اولیه
۱۵۶	۷-۱-۲ احراز هویت NTLM
۱۵۸	۷-۱-۳ CIFS آفرسکو و احراز هویت NTLM
۱۵۸	۷-۱-۴ احراز هویت NTLM passthru در آفرسکو
۱۵۹	۷-۱-۵ احراز هویت Kerberos
۱۶۲	۷-۱-۶ ورود کاربر و سرویس از طریق KDC AS
۱۶۳	۷-۱-۷ دسترسی به آفرسکو از طریق KDC TGS
۱۶۴	۷-۲ احراز هویت LDAP
۱۶۷	۷-۲-۱ هک کردن مکانیزم SLSA پشتیبانی از سرور LDAP
۱۶۷	۷-۲-۲ هماهنگ‌سازی LDAP
۱۶۸	۷-۳ احراز هویت آفرسکو و هماهنگ‌سازی زیرسیستم‌ها
۱۶۹	۷-۴ احراز هویت آفرسکو و منطقه‌های کاربردی
۱۷۰	۷-۵ تنظیمات احراز هویت و هماهنگ‌سازی با Remote Directory Server
۱۷۱	۷-۶ پیکربندی احراز هویت و هماهنگ‌سازی در برابر OpenLDAP
۱۷۱	۷-۶-۱ پیکربندی احراز هویت کاربر با OpenLDAP
۱۷۴	۷-۶-۲ پیکربندی کاربر و گروه هماهنگ شده با LDAP
۱۷۸	۷-۷ پیکربندی احراز هویت و هماهنگ‌سازی در برابر Microsoft Active Directory
۱۷۹	۷-۷-۱ پیکربندی چندگانه زیرسیستم احراز هویت LDAP

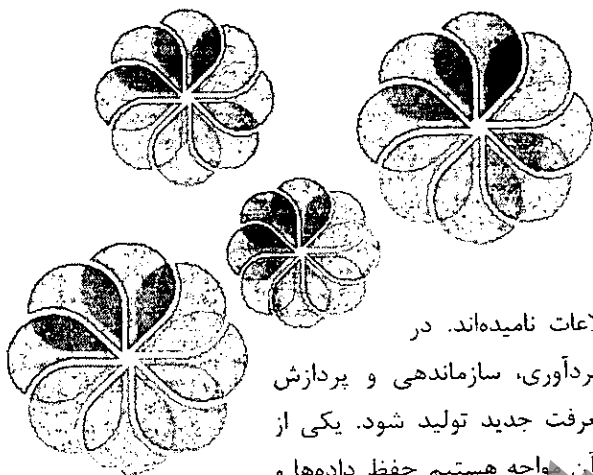
۱۸۰	انتقال پیکربندی زیرسیستم OpenLDAP به دایرکتوری خود
۱۸۰	پیکربندی احراز هویت و هماهنگ‌سازی با Active Directory
۱۸۳	شخصی‌سازی واردات گروه
۱۸۳	دسترسی از طریق رابط کاربری CIFS
۱۸۳	پیاده‌سازی یک تأییدکننده سفارشی برای احراز هویت CIFS در برابر یک سرور LDAP
۱۸۶	افزودن sambaSamAccount به ساختار LDAP
۱۸۷	تولید رمز عبور MD4
۱۸۷	ایجاد یک تأییدکننده سفارشی NTLM
۱۹۰	احراز هویت سفارشی پیکربندی زیر سیستم
۱۹۲	گسترش کلاس‌های مورد نیاز برای تأیید اعتبار سفارشی
۱۹۳	تست تأیید اعتبار سفارشی جدید
۱۹۳	احراز هویت امن‌تر و به کارگیری SSO
۱۹۵	رفع مشکل احراز هویت NTLM و SSO

فصل هشتم: مدیریت امنیت در آلفرسکو

۱۹۸	۸-۱ سناریو اول
۱۹۸	۸-۲ سناریو دوم
۱۹۹	۸-۳ سناریو سوم
۱۹۹	۸-۴ انتقال کاربران موجود به آلفرسکو
۱۹۹	۸-۴-۱ استفاده از خط فرمان اسکریپت برای آپلود کاربران
۲۰۰	۸-۵ راه‌اندازی مخزن آلفرسکو با داده کاربری از پیش تعریف شده
۲۰۰	۸-۵-۱ اجازه دسترسی
۲۰۱	۸-۵-۲ منطقه‌ها
۲۰۱	۸-۵-۳ برنامه‌های وابسته به منطقه‌ها
۲۰۲	۸-۶ دسترسی به لیست کنترل
۲۰۲	۸-۶-۱ مثالی از ACL

۲۰۳	 ۸-۷ سرویس‌های عمومی
۲۰۴	 ۸-۸ استفاده سرور دایرکتوری در Development Environment
۲۰۶	 ۸-۹ تنظیم مالکان یا Owners
۲۰۶	 ۸-۱۰ اضافه کردن مجوزها
۲۰۹	 ۸-۱۰-۱ چگونگی ایجاد مجوزها
۲۱۰	 ۸-۱۱ مدیریت عملیات (Action Management)
۲۱۱	 ۸-۱۱-۱ گرفتن تعاریف عمل
۲۱۲	 ۸-۱۱-۲ اقدامات پیش‌فرض
۲۱۳	 ۸-۱۱-۳ گرفتن یک تعریف عملیات
۲۱۴	 ۸-۱۱-۴ اجرای عمل
۲۱۵	 ۸-۱۱-۵ ذخیره عمل
۲۱۶	 ۸-۱۱-۶ دریافت عمل
۲۱۸	 ۸-۱۱-۷ حذف عمل
۲۱۹	 ۸-۱۲ مدیریت قوانین
۲۱۹	 ۸-۱۲-۱ شرایط پیش‌فرض
۲۲۱	 ۸-۱۲-۲ افزودن قوانین

پیشگفتار



دوران ما را به درستی عصر اطلاعات نامیده‌اند. در اندیشه ما، فناوری اطلاعات به مفهوم گردآوری، سازماندهی و پردازش داده‌های خام است به گونه‌ای که از آن معرفت جدید تولید شود. یکی از اساسی‌ترین مسائلی که در دنیای امروز با آن مواجه هستیم حفظ داده‌ها و اسناد و همچنین مدیریت آنان است. نرم‌افزار آلفرسکو قدرتی بی‌نظیر به سازمان می‌دهد تا اسناد خود را مدیریت کنید. این نرم‌افزار پایگاهی قابل دسترسی از طریق وب می‌سازد و امکان دسترسی مشروط را فراهم می‌آورد. از دیگر خصوصیات آلفرسکو می‌توان به کاهش هزینه‌ها، سرعت بخشیدن به کارها و امنیت بالای آن اشاره کرد. همچنین آلفرسکو می‌تواند با سیستم‌های دیگر و شبکه‌های تحت ویندوز و لینوکس که دارای سیستم احراز هویتی همچون Active Directory هستند نیز ارتباط برقرار کند به گونه‌ای که به اطلاعات کاربران در آن مکان‌ها نیز دسترسی داشته باشد و بتواند کاربران آنان را مدیریت کند.

با اینکه مدت زمان زیادی (در سال ۲۰۰۵ میلادی) از حضور آلفرسکو نمی‌گذرد، تمامی خصوصیات این سیستم محتوایی متن باز باعث شده است که در حال حاضر آلفرسکو به عنوان بزرگ‌ترین شرکت مدیریت محتوایی متن باز در جهان شناخته شود آن چنانکه تاکنون حدود ۳ میلیون دانلود، بیش از ۱۴۰۰ مشتری از ۴۳ کشور در جهان و ۱۵ میلیون سند را داراست.

در این کتاب به بیان مدیریت امنیت در سیستم مدیریت محتوایی سازمانی آلفرسکو پرداخته خواهد شد. همچنین این کتاب فرصت ایده‌آلی برای آشنایی با سیستم مدیریت محتوایی درون سازمانی آلفرسکو خواهد بود که بدین منظور مختصری از ویژگی‌های این سیستم و نحوه نصب که در فصل نخست آورده شده است، می‌پردازد. در ادامه فصل دوم و سوم به ترتیب شامل تشریح پیاده‌سازی آلفرسکو و و بررسی این پیاده‌سازی در صفحه Alfresco Share قرار خواهیم داد. در فصل چهارم با مدیریت نقش‌ها و مجوزها آشنا خواهیم شد و سپس در فصل پنجم به بررسی مجوزها در Alfresco Share خواهیم پرداخت. فصل ششم احراز هویت در آلفرسکو را مورد مطالعه قرار می‌دهیم، همچنین فصل هفتم نیز به احراز هویت در سیستم‌های مختلفی که با آلفرسکو در رابطه‌اند خواهیم پرداخت و در

نهایت فصل هشتم مدیریت امنیت در آلفرسکو را تشکیل خواهد داد. همچنین در خصوص پنج نقش درون‌ساز در این سیستم به مفسر پرداخته خواهد شد. برای بیان هر چه صریح‌تر مدل‌های امنیتی، اجازه دسترسی، پسوردها، اجازه پیاده‌سازی، مجوزها و قانون‌های به کار گرفته شده که همگی امنیت در سیستم آلفرسکو را شامل می‌شوند، یک سیستم بانک را مورد بررسی قرار داده‌ایم. تا برای علاقمندان از مبتدی تا متخصصین حرفه‌ای مفید واقع شود.

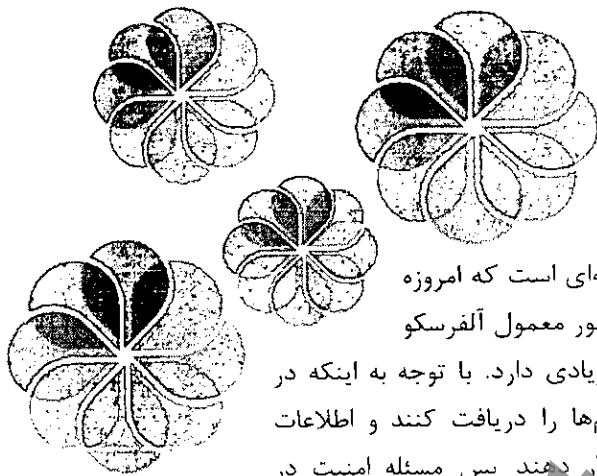
امید آن داریم تا با مطالعه هرچه بیشتر و دقیق‌تر بر روی این سیستم محتوایی که از امنیت قابل توجه و مناسبی نیز برخوردار است، در راستای مدیریت محتوا در نظام اقتصادی کشور مورد استفاده قرار گیرد تا به جای استفاده از روش‌های منسوخ شده در دنیای امروز با استفاده از آلفرسکو بتوان کارایی پویاتری را در ایران فراهم آورد.

کوشیده‌ایم که روانی و صحت مطالب را سرلوحه کار خویش قرار دهیم ولی به حکم آنکه انسان جایز الخطاست، پیشاپیش از خطاهای احتمالی پوزش می‌طلبیم و انتقادات و پیشنهادات خوانندگان محترم را به بر دیده منت خواهیم گزارد.

www.aalfresco.blogfa.com
 mostafa.amini@yahoo.com
 maryam.rezaee84@gmail.com

با سپاس

مقدمه



امنیت و مجوزهای دسترسی دغدغهای است که امروزه بسیاری از کاربران با آن مواجه هستند. به طور معمول آلفرسکو برنامه‌ای است که به کاربرانش دسترسی زیادی دارد. با توجه به اینکه در آلفرسکو کاربران می‌توانند بسیاری از فرم‌ها را دریافت کنند و اطلاعات معتبر و شخصی خود را بر روی آن قرار دهند پس مسئله امنیت در آلفرسکو هم برای یک مدیر و هم برای یک کاربر معمولی از اهمیت ویژه‌ای برخوردار است چرا که یک مدیر باید بتواند به کاربران خود این اطمینان را بدهد که از اطلاعات آنان به خوبی نگهداری می‌شود و هرگز هکرها نمی‌توانند این اطلاعات را سرقت کنند و از این اطلاعات سوء استفاده کنند.

سیستم آلفرسکو یک سیستم مدیریت سازمانی متن باز^۱ است که وسعت و امنیت جزو اصلی‌ترین خصوصیات این سیستم می‌باشد که نه تنها توانایی حفظ هزاران اسناد را در خود دارد بلکه می‌تواند با سیستم‌های دیگر و شبکه‌های تحت ویندوز و لینوکس که دارای سیستم احراز هویتی همچون Active Directory هستند نیز ارتباط برقرار کند به گونه‌ای که به اطلاعات کاربران در آن مکان‌ها نیز دسترسی داشته باشد و بتواند کاربران آنان را مدیریت کند.

به طور کلی امنیت در آلفرسکو شامل مدل‌های امنیتی، اجازه دسترسی، پسوردها، اجازه پیاده‌سازی، مجوزها و قانون‌های به کار گرفته شده می‌باشند. اجازه دسترسی در سیستم مدیریت محتوایی آلفرسکو مدل‌های زیاد و متنوعی را شامل می‌شود که از جمله می‌توان به محبوب‌ترین این مدل‌ها یعنی Access Control List اشاره کرد و مجوزها شامل افراد یا گروه‌ها می‌باشند که مشخص می‌کنند که یک فرد و یا گروه اجازه دسترسی به چه افراد و یا محتوایی را دارد. این مجوزها به صورت پیش‌فرض برای تمامی افراد سیستم اعمال خواهد شد. فرزندان به صورت مستقیم و یا با واسطه مجوزها را دریافت می‌کنند که تمامی این مجوزها از قوانین داخلی آلفرسکو تبعیت می‌کنند که البته مدیر می‌تواند به منظور امنیت بخشیدن بیشتر به کاربری، مجوز خاصی را به صورت دستی برای آن

۱ نرم‌افزار متن باز یعنی کدی که نرم‌افزار با آن تولید شده در اختیار عموم قرار داشته باشد و هر کسی بتواند آزادانه از آن کد استفاده کند و آن را تغییر دهد.

اعمال کند که به‌طور پیش‌فرض مجوزهای تنظیم شده همیشه بر مجوزهای والد اولویت دارند که این روش، راهکار بسیار مناسبی برای تضمین امنیت در این سیستم می‌باشد.

دسترسی‌ها، مجوزها و پسوردها بر روی کاربران و گروه‌ها در صفحات Alfresco Explorer و Alfresco Share و همچنین در محیط سایت آلفرسکو به چگونگی استفاده از سیستم آلفرسکو در یک محیط امن برای استفاده‌کنندگان اعم از یک مدیر و یا یک کاربر معمولی در سیستمی که به عنوان مثال آورده شده است تشریح خواهد شد. در خصوص مباحث پیشرفته در مورد امنیت بر روی این سیستم همچون استفاده از LDAP و NTUM که یک موتور سرمایه‌گذار خارجی برای احراز هویت می‌باشد نیز بررسی‌ها صورت گرفته است.