Werken met Oracle's Internet Directory

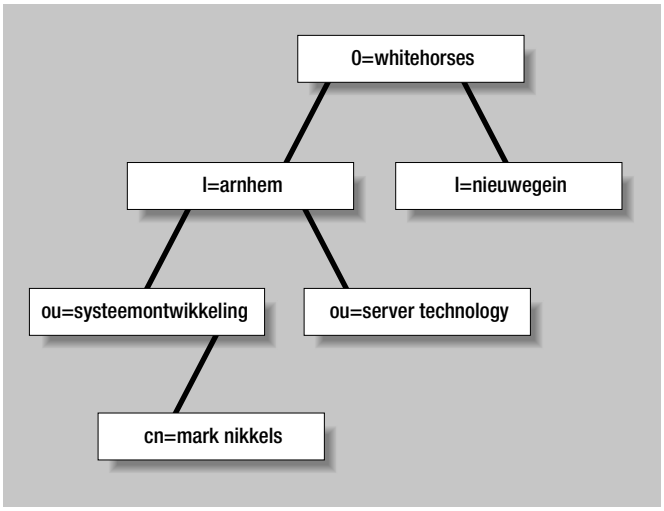
OID is spil in Oracle's mid-tier architectuur

Oracle Internet Directory (OID) is voor velen een ietwat onbekend onderdeel van de Oracle Application Server. OID vormt echter al jaren de spil in Oracle's strategie voor database gebaseerde LDAP directory services. Maar wat is nu precies LDAP, wat is OID en wat kunnen we ermee? In dit artikel lichten we alvast een tipje van de sluier op. In de komende editie van Optimize zullen we verder ingaan op het gebruik van OID en Single Sign-On voor Forms9i applicaties.

Oracle is al in 1997 begonnen met de integratie van LDAP in de diverse producten. Omdat er geen geschikte LDAP server gevonden werd startte Oracle met de bouw van Oracle Internet Directory. OID werd in 1998 voor het eerst aan klanten getoond en werd gebundeld met Oracle8i. OID is uitgegroeid tot een belangrijk onderdeel van Oracle Application Server. Het wordt onder andere gebruikt voor het centraal vastleggen van gebruikers accounts en groepsinformatie. Het belang van OID wordt geïllustreerd door het grote aantal Oracle producten dat met OID werkt, zoals Oracle Portal, Oracle Developer, Advanced Security Option van de database server, Oracle Net, Oracle Advances Queueing, Collaboration suite en Oracle's eBusiness Suite.

LDAP

LDAP staat voor Lightweight Directory Access Protocol en is het standaardprotocol voor het benaderen van een Directory. Directory's worden gebruikt voor het beheren, beveiligen en toegankelijk maken van informatie over entiteiten zoals personeelsleden, componenten van het bedrijfsnetwerk of metadata van een bedrijfsapplicatie. Een directory die met behulp van LDAP toegankelijk is noemen we een LDAP directory. Iedere entiteit heeft een corresponderende entry in de LDAP directory. Iedere entry bevat verschillende stukjes informatie, die we attributes of property's noemen. De LDAP entry's zijn in het algemeen beperkt in omvang. Een LDAP directory kent meestal maar weinig mutaties en veel opvragingen.



Figuur 1. Een grafische weergave van een Directory Information Tree

LDAP is zeer geschikt om "thin" Internet client applicaties te ondersteunen zoals Webforms9i en Oracle9iAS Portal en is gebaseerd op een eerdere ISO X.500 directory service standaard. De laatste officiële LDAP standaard is versie 3 en deze is als Internet standaard uitgeroepen in december 1997 door de Internet Engineering Task Force (IETF): de organisatie die ook verantwoordelijk is voor de welbekende Internet standaarden voor HTML, DNS en TCP/IP. Het LDAP protocol beschrijft een viertal aspecten van de entry's: naamgeving, betekenis, toegestane operaties en beveiliging. In het hierna volgende zullen deze aspecten nader worden toegelicht.

OID wordt onder andere gebruikt voor het centraal vastleggen van gebruikers accounts en groepsinformatie

1. Naamgeving

Het LDAP naming model schrijft de naamgeving van de LDAP entry's voor. Dit gebeurt zodanig dat de entry's georganiseerd kunnen worden in een zogenaamde directory information tree (DIT). Elke entry in de Directory wordt uniek geïdentificeerd met een distinguished name (DN). De distinguished name geeft de exacte plaats van de entry weer in de hiërarchie van de Directory en wordt gebruikt om aan deze entry te refereren. Een voorbeeld van een DN is:

```
cn=mark nikkels, ou=systeemontwikkeling, l=arnhem, o=whitehorses
```

Hierbij staat cn voor common name, ou voor organisational units, l voor location en o voor organisation. In het algemeen wordt de 'laagste' DIT component links in de DN geschreven, gevolgd door het volgende hogere component net zolang tot-dat het root niveau bereikt is. Om nu deze entry van buitenaf te benaderen moet de volledige en exacte DN opgegeven worden. Een voorbeeld van een DIT behorende bij deze DN wordt in figuur 1 weergegeven.

Naast de DN kent elke directory entry ook een Relative Distiguished Name (RDN). De RDN is het meest linkse gedeelte van de DN. In figuur 1 is de RDN "cn=mark nikkels".

2. Betekenis

De entry's in de DIT kunnen verschillende zaken beschrijven, zoals personeelsleden van een bedrijf, gedeelde netwerk-componenten zoals printers en file servers of bijvoorbeeld database connect descriptors (tnsnames gegevens) van de Oracle databases. Het LDAP information model beschrijft wat er per type entry wordt vastgelegd.

Zo zal men bij een personeelslid bijvoorbeeld willen vastleggen: voornaam, achternaam, geboortedatum, zakelijk e-mailadres, privé e-mailadres, pasfoto. Maar voor een database connect descriptor entry wordt natuurlijk iets anders vastgelegd, bijvoorbeeld protocol, host en port.

Zoals we al beschreven kent iedere directory entry één of meer attributes waarin de informatie wordt vastgelegd. Een attribute wordt gekenmerkt door een attribute type en eventueel één of meer toegestane attribute values, bijvoorbeeld de toegestane waarden voor een locatie. OID werkt met object classes, die één of meer attributes bevatten. Het definiëren van attributes voor een entry gebeurt door het toewijzen van één of meer object classes aan deze entry. Object classes werken met overerving, waardoor eenvoudig nieuwe object classes kunnen worden samengesteld uit één of meer andere object classes.

3. Toegestane operaties

Het functional model bepaalt welke operaties zijn toegestaan op een entry in de DIT. Er zijn een aantal LDAP functies mogelijk: zoeken, lezen, wijzigen en authenticeren. De leesoperatie haalt één of meer entry's op of leest de attributes van een bepaalde entry. De zoekoperatie zoekt met behulp van een zoekfilter in de gehele DIT of in een bepaald gedeelte van de DIT. De wijzigoperatie kan de naam van entry's of de inhoud van de attributes wijzigen, entry's toevoegen of entry's verwijderen. De authenticatieoperatie tenslotte stelt een client sessie in staat om één of meer operaties op de DIT uit te voeren nadat de cliëntsessie succesvol geïdentificeerd is.

4. Beveiliging

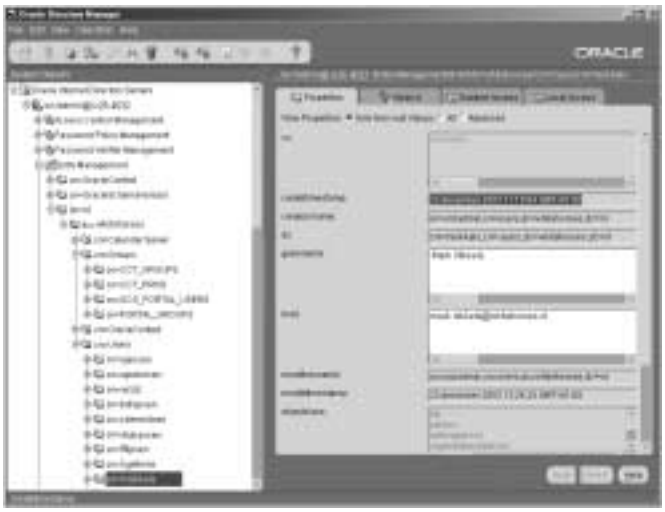
Het security model regelt de beveiliging van de informatie in de DIT, gaat in op de wijze van authenticatie (dit kan zijn: anoniem, met behulp van wachtwoord, of met behulp van Secure Socket Layers) en bepaalt wat een gebruiker wel en niet mag lezen of wijzigen. Tot slot beschrijft het security model hoe de LDAP gegevens afgeschermd verstuurd worden, hoe de versleuteling van de opgeslagen wachtwoorden moet plaatsvinden en welke regels (policy's) gelden voor het wijzigen van de opgeslagen wachtwoorden.

Informatie in een LDAP directory, kan door diverse LDAP clients worden benaderd, waaronder bijvoorbeeld ook Microsoft Outlook. Dit toont direct de meerwaarde van een LDAP server in een Oracle omgeving, waar alle gegevens toch al centraal worden vastgelegd. Door het opslaan van gebruikers-, applicatie- en netwerkgegevens in OID wordt het mogelijk om deze informatie te delen met andere, ook niet-Oracle, LDAP clients.

Database accounts?

Het inzetten van OID betekent een wijziging in de traditionele Oracle applicatiearchitectuur. Het vastleggen van de applicatie-gebruikers en rollen (groepen) vindt niet meer, zoals dat voorheen meestal gebeurde, plaats in de database, maar in OID. Op één centrale plaats worden gebruikers en groepen geregistreerd om vervolgens gedeeld te worden door meerdere applicaties, bijvoorbeeld Oracle Portal, Forms9i en Collaboration Suite. In deze opzet loggen gebruikers dus niet meer in op de database, maar maken gebruik van OID. Het inloggen op OID gebeurt met behulp van Oracle's Single Sign-On (SSO) dat onderdeel is van de Oracle Application Server. Nadat SSO de inloggegevens succesvol gecontroleerd heeft met behulp van OID, krijgt de gebruiker toegang tot de bedrijfsapplicaties die geregistreerd zijn in OID.

Het belang van database accounts neemt hierdoor aanzienlijk af. Een Oracle applicatie (bijvoorbeeld gebouwd met Forms9i) zal daarom naast een databaseschema nog slechts één of hooguit



Figuur 2. Oracle Directory Manager

enkele database accounts benodigd hebben. Door de introductie van OID wordt het beheren van de applicatiegebruikers van de databaselaag verschoven naar de applicatielaag. Oracle spreekt in deze opzet dan ook van "enterprise" users en roles in tegenstelling tot "database" user en roles, omdat een in OID registreerde gebruiker immers tot meerdere applicaties en databases toegang kan hebben.

Migratie naar OID

Bij het overzetten van een 'traditionele' Oracle applicatie met database users naar een applicatie omgeving met OID dienen de database users en groepen geheel of gedeeltelijk overgezet te worden naar OID. Gekozen kan worden tussen een meerdere scenario's:

1. *Gehele migratie* – alle database gebruikers en rollen worden overgezet naar OID gebruikers en groepen. Alle applicatiegebruikers maken gebruik van een algemene databasegebruiker ten behoeve van de benodigde databaseconnectie. Deze algemene databasegebruiker heeft toegang tot alle applicatiegegevens. De applicatie werkt intern met de OID gebruikersnaam.
2. *Gedeeltelijke migratie* – de database gebruikers worden overgezet naar OID, maar de database rollen blijven bestaan in de database. De database rollen worden selectief aangezet - bijvoorbeeld met de database package dbms_session.set_role(). Op deze wijze blijven de applicatiegegevens afgeschermd bij de directe database toegang – dus buiten de applicatie om.
3. *Geen migratie* – alle database gebruikers krijgen een corresponderende OID gebruiker. Dit scenario is mogelijk omdat per gebruiker in OID wordt aangegeven welke database connectie worden moeten opgezet voor de applicatie. Alles blijft dus bij hetzelfde, alleen ontstaat er een dubbele gebruikers administratie.

Bij bovenstaande migratiescenario's moet de kanttekening worden gemaakt dat het inzetten van OID vooral kostenbesparend gaat werken indien er zoveel mogelijk applicaties gebruik van maken. En indien een zo groot mogelijk deel van de gebruikersadministratie wordt overgeheveld naar OID.

Het werken met OID

Oracle Internet Directory is onderdeel van de Oracle Application Server waarbij de DIT opgeslagen wordt in de Infrastructure database. Oracle biedt naast het LDAP protocol een aantal verschillende mogelijkheden om OID te benaderen.

Oracle Directory Manager

De belangrijkste tool voor de OID beheerder is de Oracle Directory Manager, waarmee de directory entry's, attributes en objectclasses worden geadministreerd en beheerd.
De Oracle Directory Manager is een grafische tool die met Java gebouwd is (zie figuur 2).

Command-line tools

Naast de Oracle Directory Manager bevat OID een aantal command-line tools waarmee de directory entry's gemanipuleerd kunnen worden.

- Met behulp van de LDAP tools kunnen directory entry's gemanipuleerd worden. Voorbeelden van de LDAP-tools zijn ´ldapadd´, ´ldapbind´, ´ldapcompare´ en ´ldapdelete´.
- Met behulp van de bulk-tools kunnen grote hoeveelheden directory entry's aangemaakt worden bijvoorbeeld met behulp van gegevens uit andere applicaties. Voorbeelden van deze bulktools zijn ´bulkload´, ´bulkmodify´, ´bulkdelete´ en ´ldifwrite´.
- Een catalog beheer tool wordt gebruikt om bestaande attributes indexeerbaar te maken.

Veel command-line tools maken gebruik van ASCII files die opgebouwd zijn met de LDAP Data Interchange Format (LDIF). LDIF is een ASCII file formaat standaard dat gebruikt wordt om LDAP gegevens uit te wisselen tussen LDAP servers.

Starten en stoppen van OID

De Oracle directory server wordt gestopt en gestart met

Oracle biedt naast het LDAP protocol een aantal verschillende mogelijkheden om OID te benaderen

behulp van de OID Control Utility (een command-line tool) of met behulp van de Oracle Enterprise Manager. Beide tools maken op hun beurt weer gebruik van de OID Monitor.
De OID monitor is een aparte tool die op aanvraag van de Control Utility of de Enterprise Manager de OID processen start of stopt.

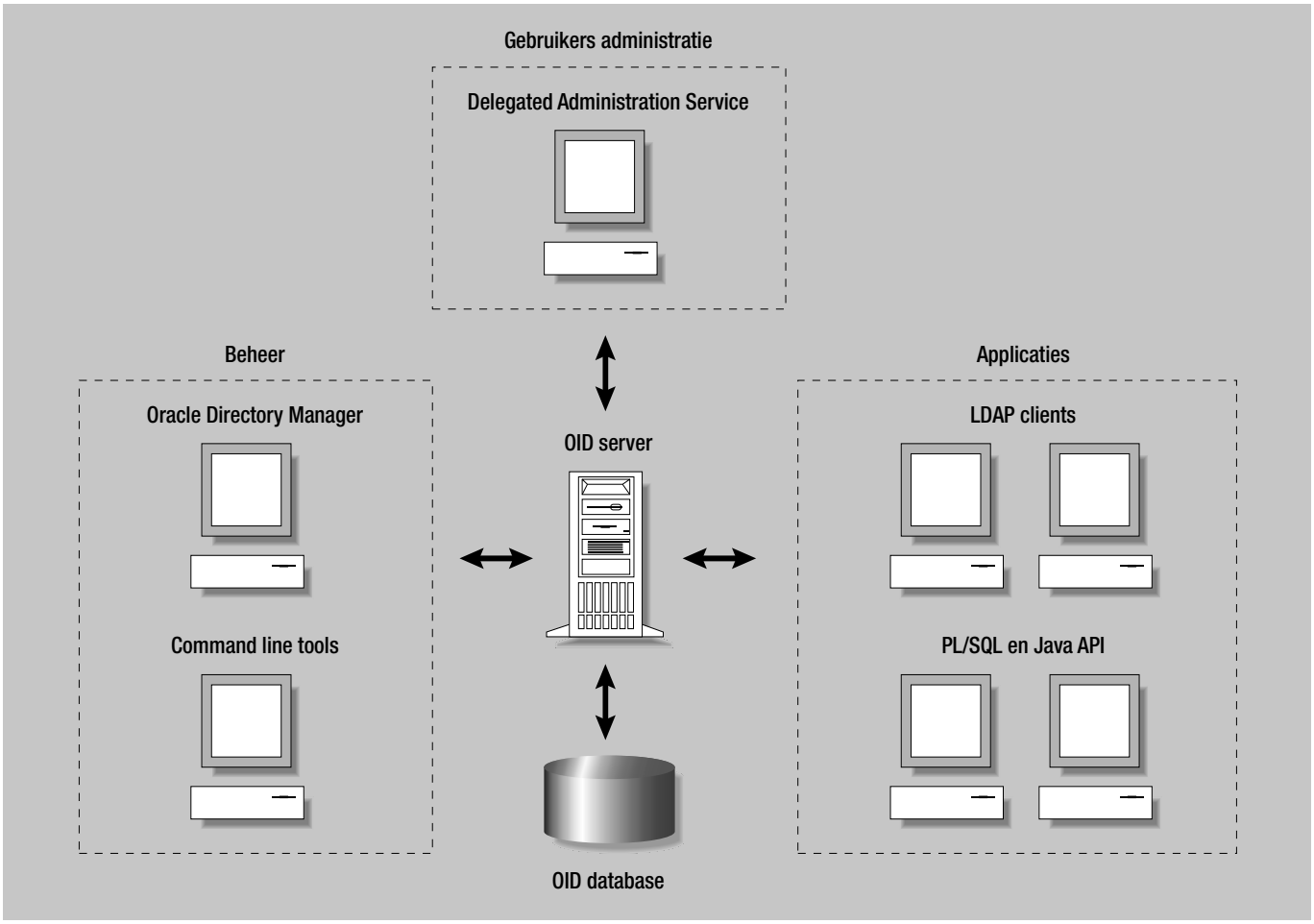
Delegated Administration Service
De Delegated Administration Service (DAS) van OID stelt eindgebruikers in staat om zelf eigen wachtwoorden te wijzigen, en geeft applicatiebeheerders de mogelijkheid om zelf gebruikers en groepen toe te voegen zonder hiervoor de OID beheerder lastig te vallen. De Delegated Administration Service maakt gebruik van Oracle Portal.

PL/SQL en Java API
De Oracle Internet directory kan worden benaderd met behulp van de DBMS_LDAP en DBMS_LDAP_UTIL PL/SQL packages of met behulp van de Java API (bijvoorbeeld de Java class frmDirectoryManager. Op deze wijze kan een directe koppeling vanuit bijvoorbeeld Oracle9i Webforms worden aangelegd, waarbij de Forms applicatie informatie opvraagt uit de Oracle Internet Directory. De PL/SQL packages bieden een 'low-level' API voor OID terwijl met behulp van de Java classes wat eenvoudiger met OID kan worden gecommuniceerd.

In onderstaande voorbeeldcode wordt geïllustreerd op welke wijze gewerkt wordt met de Dbms_Ldap en de Dbms_Ldap_Util packages om informatie uit de Oracle Internet directory te lezen.

```
Declare
  Ldap_Host           Varchar2(256);
  Ldap_Port           Pls_Integer;
  Ldap_User           Varchar2(256);
  Ldap_Passwd         Varchar2(256);
  Ldap_Base           Varchar2(256);

  Retval              Pls_Integer;
  My_Session          Dbms_Ldap.Session;

  Subscriber_Handle   Dbms_Ldap_Utl.Handle;
  Sub_Type            Pls_Integer;
  Subscriber_Id       Varchar2(2000);

  My_Pset_Coll        Dbms_Ldap_Utl.Property_Set_Collection;
  My_Property_Names   Dbms_Ldap.String_Collection;
  My_Property_Values Dbms_Ldap.String_Collection;

  User_Handle         Dbms_Ldap_Utl.Handle;
  User_Id             Varchar2(2000);
  User_Type           Pls_Integer;
  User_Password       Varchar2(2000);

  My_Mod_Pset         Dbms_Ldap_Utl.Mod_Property_Set;
  My_Attrs            Dbms_Ldap.String_Collection;
```

```
Begin
  ------------------------------
  -- connect to the ldap server and obtain and ld session.
  ------------------------------
  Ldap_Host   := 'lx25.whitehorses.nl' ;
  Ldap_Port   := 4032;
  My_Session  := Dbms_Ldap.Init(Ldap_Host,Ldap_Port);
  ------------------------------
  -- bind to the directory
  ------------------------------
  Ldap_User   := 'cn=orcladmin';
  Ldap_Passwd := 'optimze';
  Retval      := Dbms_Ldap.Simple_Bind_S
                      (My_Session,Ldap_User,Ldap_Passwd);
  ------------------------------------
  -- create subscriber handle
  ------------------------------------
  Sub_Type      := Dbms_Ldap_Utl.Type_Dn;
  Subscriber_Id := 'dc=whitehorses,dc=nl';
  Retval        := Dbms_Ldap_Utl.Create_Subscriber_Handle
                       (Subscriber_Handle,Sub_Type,Subscriber_Id);
  ------------------------------------
  -- create user handle
  ------------------------------------
  User_Type := Dbms_Ldap_Utl.Type_Dn;
  User_Id := 'cn=portal92,cn=users,dc=whitehorses,dc=nl';
  Retval :=
Dbms_Ldap_Utl.Create_User_Handle(User_Handle,User_Type,User_Id);
  ------------------------------------
  -- set user handle properties (link subscriber to user )
  ------------------------------------
  Retval := Dbms_Ldap_Utl.Set_User_Handle_Properties

(User_Handle,Dbms_Ldap_Utl.Subscriber_Handle,Subscriber_Handle);
  ------------------------------------
  -- retrieve user properties
  ------------------------------------
  My_Attrs(1) := 'cn';
  Retval := Dbms_Ldap_Utl.Get_Group_Membership
    (My_Session,User_Handle,Dbms_Ldap_Utl.Nested_Membership
    ,My_Attrs,My_Pset_Coll);
  ------------------------------------
  -- print properties obtained for the user.
  ------------------------------------
  If My_Pset_Coll.Count > 0
  Then
    For i In My_Pset_Coll.First .. My_pset_coll.last
    Loop
      Retval := Dbms_Ldap_Utl.Get_Property_Names
                  (My_Pset_Coll(i),My_Property_Names);
      If My_Property_Names.Count > 0
      Then
        For j In My_Property_Names.First .. My_property_names.Last
        Loop
          Retval := Dbms_Ldap_Utl.Get_Property_Values

(My_Pset_Coll(i),My_Property_Names(j),My_Property_Values);
          If My_Property_Values.Count > 0 Then
            For K In My_Property_Values.First..My_Property_Values.Last
            Loop
             ...
            End loop;
          End If; -- my_property_values.count > 0
        End Loop;
      End If; -- my_property_names.count > 0
    End Loop;
  End If; -- if my_pset_coll.count > 0
...
```



Figuur 3. De OID architectuur

Figuur 3 geeft de samenhang tussen de verschillende Oracle Internet Directory componenten weer.

Distributed directories

Ondanks het feit dat een LDAP directory een centrale informatiebron is kan deze fysiek gedistribueerd worden over meerdere servers. Door deze distributie wordt de hoeveelheid werk die een individuele server moet verrichten gedeeld met andere servers. Een gedistribueerde directory kan gerepliceerd worden of gepartitioneerd, of een combinatie van beide. Bij replicatie worden de directory entry's door meerdere servers redundant opgeslagen. Bij partitionering worden de directory entry's verdeeld over de directory servers. Het distribueren van de directory entry's vindt plaats met de Oracle directory replication server, waarbij een volledige DIT of een gedeelte van de DIT gerepliceerd kan worden.

Conclusie

Oracle Internet Directory vormt een zeer belangrijk onderdeel van Oracle's huidige mid-tier architectuur en is daarom niet meer weg te denken in moderne Oracle applicatie omgevingen. Voor nieuwe applicaties is het gebruik van OID dan ook sterk aan te raden.

Bij het inzetten van Oracle Internet Directory voor bestaande applicaties, moet een migratie van database accounts naar OID accounts worden overwogen. De gebruikers- en groepsinformatie kan dan worden gedeeld over meerdere applicaties. OID kan kostenbesparend werken indien men er in slaagt om meerdere (Oracle) applicaties aan te sluiten op dezelfde Oracle Internet Directory.

Rudolf Beekman en Mark Nikkels
zijn senior consultants bij Whitehorses.
E-mail: rudolf.beekman@whitehorses.nl en mark.nikkels@whitehorses.nl.