Berechtigungsreports / Prüfungsfragen

Bereich AD/WinNt

#206 Welcher AD-User hat sich länger als X Tage nicht mehr angemeldet?

Zeigt alle User an, die vor mehr als X Tagen zum letzten Mal das Passwort gewechselt haben.

#207 Welcher WinNT-User hat eine längere Passwortwechselzeit als X Tage?

Zeigt alle WinNT-User an, deren Passwort-Wechsel-Zeit länger als X Tage ist.

#208 Welcher akt. AD-User hat sich länger als X-Tage nicht mehr ang, o. das PW gew.?

Zeigt alle User an, die vor mehr als X Tagen zum letzten Mal das Passwort gewechselt oder sich zum letzten Mal angemeldet haben und deren Konto aktiv ist. Gesperrte Konten und Konten, deren Passwort nie abläuft, werden nicht angezeigt.

#210 Bei welchen AD-Kennungen läuft das Passwort nicht ab?

Zeigt alle Kennungen im AD an, bei denen das Passwort nicht geändert werden muss.

SCRIPT - Das Anmeldeskript wird ausgeführt.

ACCOUNTDISABLE - Das Benutzerkonto wird deaktiviert.

HOMEDIR_REQUIRED - Basisverzeichnis erforderlich.

PASSWD_NOTREQD - Es ist kein Kennwort erforderlich.

PASSWD_CANT_CHANGE - Der Benutzer kann das Kennwort nicht ändern. Dies ist eine Berechtigung für das Objekt des Benutzers. Informationen zur Festlegung dieser Berechtigung per Programm finden Sie auf folgender Website: (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adsi/adsi/modifying_user_cannot_change_password_ldap_provider.asp)

ENCRYPTED_TEXT_PASSWORD_ALLOWED - Der Benutzer kann ein verschlüsseltes Kennwort senden.

TEMP_DUPLICATE_ACCOUNT - Konto für Benutzer, deren primäres Konto sich in einer anderen Domäne befindet. Dieses Konto gewährt den Zugriff des Benutzers auf diese Domäne, jedoch nicht auf Domänen, die dieser Domäne vertrauen. Dies wird manchmal als "lokales Benutzerkonto" bezeichnet.

NORMAL_ACCOUNT - Standardkontotyp für einen typischen Benutzer.

INTERDOMAIN_TRUST_ACCOUNT - Konto für ein Vertrauenskonto einer Domäne, die anderen Domänen vertraut.

WORKSTATION_TRUST_ACCOUNT - Computerkonto für einen Computer mit Microsoft Windows NT 4.0 Workstation, Microsoft Windows NT 4.0 Server, Microsoft Windows 2000 Professional oder Windows 2000, der Mitglied dieser Domäne ist.

SERVER_TRUST_ACCOUNT - Computerkonto für einen Domänencontroller, der Mitglied dieser Domäne ist.

DONT_EXPIRE_PASSWD - Kennwort, das für dieses Konto nie ablaufen sollte.

MNS_LOGON_ACCOUNT - "Majority Node Set" (MNS) Anmeldekonto. Mit MNS kann man einen "Multi-Node Windows Cluster" konfigurieren, ohne eine "Common Shared Disk" zu verwenden.

SMARTCARD_REQUIRED - Wenn dieses Kennzeichen gesetzt ist, wird der Benutzer gezwungen, sich über eine Smartcard anzumelden.

TRUSTED_FOR_DELEGATION - Wenn dieses Kennzeichen gesetzt ist, wird dem Dienstkonto (dem Benutzer- oder Computerkonto), unter dem ein Dienst ausgeführt wird, für Kerberos-Delegierungszwecke vertraut. Jeder derartige Dienst kann die Identität eines Clients annehmen, der den Dienst anfordert. Sie müssen dieses Flag für die Eigenschaft userAccountControl des Dienstkontos setzen, um einen Dienst für die Kerberos-Delegierung zu aktivieren.

NOT_DELEGATED - Wenn dieses Kennzeichen gesetzt ist, wird der Sicherheitskontext des Benutzers nicht an einen Dienst delegiert, auch dann nicht, wenn das Dienstkonto als "für Delegierungszwecke vertraut" definiert ist.

USE_DES_KEY_ONLY - (Windows 2000/Windows Server 2003) Beschränken Sie diesen Prinzipal auf DES-Verschlüsselungstypen für Schlüssel (DES = Data Encryption Standard).

Berechtigungsreports / Prüfungsfragen

Bereich AD/WinNt

#210 Bei welchen AD-Kennungen läuft das Passwort nicht ab?

DONT_REQUIRE_PREAUTH - (Windows 2000/Windows Server 2003) Dieses Konto setzt keine Kerberos-Vorauthentifizierung für die Anmeldung voraus.

PASSWORD_EXPIRED - (Windows 2000/Windows Server 2003) Das Kennwort des Benutzers ist abgelaufen.

TRUSTED_TO_AUTH_FOR_DELEGATION - (Windows 2000/Windows Server 2003) Dem Konto wird für Delegierungszwecke vertraut. Dies ist eine sicherheitskritische Einstellung. Konten, bei denen diese Option aktiviert ist, sollten genau kontrolliert werden. Diese Einstellung ermöglicht einem Dienst, der unter diesem Konto ausgeführt wird, die Identität des Clients anzunehmen

#211 Welche AD-Kennungen können sich ohne Passwort anmelden?

Zeigt alle Kennungen im AD an, bei denen das Passwort "leer" sein kann. Meist sind diese Konten über Smartcards abgesichert (Anmeldung nur über Smartcard möglich - SMARTCARD_REQUIRED)

SCRIPT - Das Anmeldeskript wird ausgeführt.

ACCOUNTDISABLE - Das Benutzerkonto wird deaktiviert.

HOMEDIR_REQUIRED - Basisverzeichnis erforderlich.

PASSWD_NOTREQD - Es ist kein Kennwort erforderlich.

PASSWD_CANT_CHANGE - Der Benutzer kann das Kennwort nicht ändern. Dies ist eine Berechtigung für das Objekt des Benutzers. Informationen zur Festlegung dieser Berechtigung per Programm finden Sie auf folgender Website: (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adsi/adsi/modifying_user_cannot_change_password_ldap_provider.asp)

ENCRYPTED_TEXT_PASSWORD_ALLOWED - Der Benutzer kann ein verschlüsseltes Kennwort senden.

TEMP_DUPLICATE_ACCOUNT - Konto für Benutzer, deren primäres Konto sich in einer anderen Domäne befindet. Dieses Konto gewährt den Zugriff des Benutzers auf diese Domäne, jedoch nicht auf Domänen, die dieser Domäne vertrauen. Dies wird manchmal als "lokales Benutzerkonto" bezeichnet.

NORMAL_ACCOUNT - Standardkontotyp für einen typischen Benutzer.

INTERDOMAIN_TRUST_ACCOUNT - Konto für ein Vertrauenskonto einer Domäne, die anderen Domänen vertraut.

WORKSTATION_TRUST_ACCOUNT - Computerkonto für einen Computer mit Microsoft Windows NT 4.0 Workstation, Microsoft Windows NT 4.0 Server, Microsoft Windows 2000 Professional oder Windows 2000, der Mitglied dieser Domäne ist.

SERVER_TRUST_ACCOUNT - Computerkonto für einen Domänencontroller, der Mitglied dieser Domäne ist.

DONT_EXPIRE_PASSWD - Kennwort, das für dieses Konto nie ablaufen sollte.

MNS_LOGON_ACCOUNT - "Majority Node Set" (MNS) Anmeldekonto. Mit MNS kann man einen "Multi-Node Windows Cluster" konfigurieren, ohne eine "Common Shared Disk" zu verwenden.

SMARTCARD_REQUIRED - Wenn dieses Kennzeichen gesetzt ist, wird der Benutzer gezwungen, sich über eine Smartcard anzumelden.

TRUSTED_FOR_DELEGATION - Wenn dieses Kennzeichen gesetzt ist, wird dem Dienstkonto (dem Benutzer- oder Computerkonto), unter dem ein Dienst ausgeführt wird, für Kerberos-Delegierungszwecke vertraut. Jeder derartige Dienst kann die Identität eines Clients annehmen, der den Dienst anfordert. Sie müssen dieses Flag für die Eigenschaft userAccountControl des Dienstkontos setzen, um einen Dienst für die Kerberos-Delegierung zu aktivieren.

NOT_DELEGATED - Wenn dieses Kennzeichen gesetzt ist, wird der Sicherheitskontext des Benutzers nicht an einen Dienst delegiert, auch dann nicht, wenn das Dienstkonto als "für Delegierungszwecke vertraut" definiert ist.

USE_DES_KEY_ONLY - (Windows 2000/Windows Server 2003) Beschränken Sie diesen Prinzipal auf DES-

Berechtigungsreports / Prüfungsfragen

Bereich AD/WinNt

#211 Welche AD-Kennungen können sich ohne Passwort anmelden?

Verschlüsselungstypen für Schlüssel (DES = Data Encryption Standard).

DONT_REQUIRE_PREAUTH - (Windows 2000/Windows Server 2003) Dieses Konto setzt keine Kerberos-Vorauthentifizierung für die Anmeldung voraus.

PASSWORD_EXPIRED - (Windows 2000/Windows Server 2003) Das Kennwort des Benutzers ist abgelaufen.

TRUSTED_TO_AUTH_FOR_DELEGATION - (Windows 2000/Windows Server 2003) Dem Konto wird für Delegierungszwecke vertraut. Dies ist eine sicherheitskritische Einstellung. Konten, bei denen diese Option aktiviert ist, sollten genau kontrolliert werden. Diese Einstellung ermöglicht einem Dienst, der unter diesem Konto ausgeführt wird, die Identität des Clients anzunehmen

#212 Bei welcheln WinNT-Kennungen läuft das Passwort nicht ab?

Zeigt alle WinNT-Kennungen an, bei denen das Passwort nie abläuft.

#213 Welcher WinNT-Passwortwechsel ist älter als X Tage?

Zeigt alle WinNT-User an, deren letzter Passwort-Wechsel länger als X Tage zurück liegt.

#214 Welche Konten sind deaktiviert oder gesperrt?

Zeigt alle AD- und WinNT-Konten an, die gesperrt oder deaktiviert sind.

#215 Bei welchen AD-Kennungen wurde das Passwort noch nie geändert?

Zeigt alle Kennungen, deren Passwort noch nie verändert wurde (Datum <= 01.01.1900)

#250 Welche AD-User haben keinen KURS-User?

Zeigt AD-User an, die in KURS keinen User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das AD-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!

#251 Welche KURS-User haben keinen AD-User?

Zeigt KURS-User an, die keinen AD-User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das AD-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!

Berechtigungsreports / Prüfungsfragen

Bereich Berechtigungen

#5 Wer hat eine bestimmte Berechtigung?

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter inklusive Feindefinitionen an, und zwar nach der OE sortiert.

Technischer User RZ erben keine Berechtigungen des Instituts oder von Stellen / OEs.

Hinweis: Der Report zeigt administrierte konkurrierende Berechtigungen farbig an, wenn sowohl die führende Berechtigung als auch die abhängige konkurrierende Berechtigung nicht durch Filterung im Report ausgeschlossen wurden.

#6 Welche Profile mit welchen Berechtigungen gibt es?

Der Report erzeugt eine Übersicht aller Profile und den darin enthaltenen Berechtigungen inkl. Kompetenzen.

#9 Wann wurden oder werden Berechtigungen entzogen?

Zeigt alle Berechtigungen, die ablaufen bzw. bereits abgelaufen sind, an. So kann man z.B. prüfen, ob Berechtigungen terminiert sind; wenn man beispielsweise das heutige Datum eingibt, sieht man, welche Profile zukünftig ablaufen.

#10 Welche Berechtigungen hängen direkt an einem MA?

In OSP ist es möglich, Mitarbeitern direkt Berechtigungen zuzuweisen (also nicht über Profile). Dieser Report zeigt alle Berechtigungen inkl. Feindefinitionen / Eigenschaften / Kompetenzen, die direkt an einen Mitarbeiter vergeben sind.

#17 Welche Profile enthalten Negierungen?

Der Report erzeugt eine Übersicht aller Profile, in denen Negierungen enthalten sind.

#23 Wann wurden oder werden einem Mitarbeiter Berechtigungen entzogen?

Zeigt alle Berechtigungen von Mitarbeitern an, die ablaufen bzw. bereits abgelaufen sind, an. So kann man z.B. prüfen, ob Berechtigungen terminiert sind, und zwar nach Namen sortiert; wenn man beispielsweise das heutige Datum eingibt, sieht man, welche Profile zukünftig ablaufen.

#31 Wer hat eine negierte Berechtigung?

Der Report zeigt alle negierten Berechtigungen einzelner Mitarbeiter an, und zwar nach der OE sortiert.

#32 Welche Kompetenzen können MA auf all ihren Stellen haben?

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter, denen Eigenschaften / Kompetenzen zugewiesen sind, an und zwar nach Eigenschaft sortiert. Zusätzlich werden pro Mitarbeiter die Eigenschaften / Kompetenzen dargestellt, die sich für Stellen des Filters 'OE-Stellen-Zuordnungsart', ergeben. Berechtigungen ohne Eigenschaften / Kompetenzen werden nicht angezeigt.

#33 Welche Profile ähneln sich?

Der Report zeigt die Anzahl der Abweichungen aller Profile untereinander an. Dadurch lassen sich Redundanzen bzw. geringfügige Abweichungen identifizieren, die dann durch Anpassung der Profile aufgehoben werden können. Der Report berücksichtigt Attribute, alle Feindefinitionen sowie alle zugewiesenen Eigenschaften.

Geben Sie hier die maximalen Anzahl der Unterschiede zwischen Profilen an, die angezeigt werden sollen. Wenn Sie 2 Profile (oder auch mehrere einzelne) vergleichen wollen, geben Sie am besten einen sehr hohen Wert für "Anzahl" an, damit die Unterschiede auch im Report aufgeführt werden.

Je höher "Anzahl" (bei Selektion aller Profile), um so länger dauert die Berechnung, da jedes Profil mit jedem verglichen wird und erst bei "Anzahl" Unterschieden der Vergleich abgebrochen wird.

Als 1 Unterschied gilt: 1 Berechtigung, 1 bis alle Attribute einer Berechtigung, 1 Feindefinition, 1 bis alle Attribute auf Feindefinitionsebene, 1 Eigenschaft

#34 Welche Berechtigung ist in einem Profil NICHT enthalten?

Der Report zeigt Profile an, in denen bestimmte Berechtigungen NICHT vorhanden sind.

#35 Welche Profile enthalten keine Berechtigung?

Der Report zeigt alle Profile an, denen überhaupt keine Berechtigungen zugeordnet sind. Es werden keine Menüprofile mit ausgegeben.

Berechtigungsreports / Prüfungsfragen

Bereich Berechtigungen

#36 Welche Profile haben weniger als X User?

Der Report zeigt Profile an, die weniger als X Mitarbeitern direkt zugewiesen sind. (OE- und Stellen-Zuweisungen werden nicht berücksichtigt)

#44 Welcher MA hat negierte und nicht negierte Berechtigungen?

Der Report zeigt Zuweisungen bestimmter Berechtigungen zu einem bestimmbaren Zeitpunkt an, die einer Person direkt oder über Vererbung (über Profil, Stelle oder OE) zugewiesen wurden. Dabei werden nur solche User angezeigt, die gleichzeitig eine Berechtigung mit Negierung und ohne Negierung erhalten. Der Report zeigt nur Mitarbeiter an, die Stellen über Rollen (z.B. HIER TÄTIG, PLANSTELLE) auch tatsächlich zugewiesen sind.

Das Institutsprofil wird hier nicht gesondert berücksichtigt, da es allen Mitarbeitern zugeschlüsselt ist (nutzen Sie hierfür ggf. Report #6).

#48 Welche Berechtigungen / Profile wurden in einem best. Zeitraum administriert?

Zeigt alle Berechtigungen, die in einem bestimmten Zeitraum vergeben wurden.

#49 Wer hat wann eine Berechtigung erhalten?

Zeigt alle Berechtigungen nach Mitarbeiternamen sortiert an, die in einem bestimmten Zeitraum vergeben wurden.

#50 Wo wurden bestimmte Profile zugewiesen?

Der Report zeigt Zuweisungen bestimmter Berechtigungen zu einem bestimmbaren Zeitpunkt an, die einer Person direkt oder über Vererbung (über Profil, Stelle oder OE) zugewiesen wurden. Der Report zeigt nur Mitarbeiter an, die Stellen über Rollen (z.B. HIER TÄTIG, PLANSTELLE) auch tatsächlich zugewiesen sind.

Das Institutsprofil wird hier nicht gesondert berücksichtigt, da es allen Mitarbeitern zugeschlüsselt ist (nutzen Sie hierfür Report #86, dort wird zusätzlich das Institutsprofil mit ausgegeben).

Der Report zeigt Zuweisungen bestimmter Berechtigungen zu einem bestimmbaren Zeitpunkt an, die einer Person direkt oder über Vererbung (über Profil, Stelle oder OE) zugewiesen wurden. Der Report zeigt nur Mitarbeiter an, die Stellen über Rollen (z.B. HIER TÄTIG, PLANSTELLE) auch tatsächlich zugewiesen sind.

Das Institutsprofil wird hier nicht gesondert berücksichtigt, da es allen Mitarbeitern zugeschlüsselt ist (nutzen Sie hierfür Report #86, dort wird zusätzlich das Institutsprofil mit ausgegeben).

#52 Welche Stelle (oder OE) hat welches Profil?

Der Report zeigt alle Zuweisungen bestimmter Profile zu einem Zeitpunkt an, die einer Person, einer Stelle oder einer OE direkt oder indirekt zugewiesen wurde.

Hinweis: Es werden nur solche Oes und Stellen angezeigt, denen auch User über die eingestellte Zuordnungsart zugewiesen sind. Wenn z.B. in den Stellen einer OE keine User zugewiesen ist, wird die OE nicht aufgeführt. Nutzen Sie dafür den Report #53.

#54 Welche Profile werden nirgends verwendet?

Der Report zeigt Profile an, die aktuell nicht verwendet werden. Es werden Berechtigungsprofile (IST), Menüprofile und Funktionsprofile (SOLL) angezeigt.

#58 Welche Berechtigunsveränderungen wurden in einem best. Zeitraum administriert?

Zeigt alle hinzugefügten und entzogenen Berechtigungen in einem bestimmten Zeitraum, nach Datum sortiert, an.

#60 Welche MA haben vollumfängliche Rechte zur Änderungsbearbeitung?

Der Report zeigt alle User an, die für das Gesamthaus (OE 0000000 bis 9999999) alle Tätigkeits-ID (00000 bis 99999) prüferisch tätig sein können (Berechtigung: AEND-BEARB). Über den OE-Stellen-Zuordnungsart kann festgelegt werden, welche Zuordnungsarten angezeigt werden.

#79 Welchen Usern wurden direkt negierte Ber. zugewiesen?

Der Report erzeugt eine Übersicht aller User, denen direkt negierte Berechtigungen zugewiesen wurden.

#81 Welche Kompetenzen haben MA auf ihrer Planstelle?

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter, bei denen Eigenschaften / Kompetenzen zugewiesen sind,

Berechtigungsreports / Prüfungsfragen

Bereich Berechtigungen

#81 Welche Kompetenzen haben MA auf ihrer Planstelle?

an und zwar nach Eigenschaft sortiert. Es wurden nur die PLANSTELLEN angezeigt. Berechtigungen ohne Eigenschaften / Kompetenzen werden nicht angezeigt.

#85 Welche Berechtigungen gibt es in den Anwendungssystemen?

Zeigt alle Berechtigungen an, die ein Anwendungssystem zur Verfügung stellt.

#87 Welche Kompetenzen wurden hinzugefügt oder entfernt?

Der Report zeigt hinzugefügte und entfernte Kompetenzen / Eigenschaften in einem bestimmten Zeitraum an.

#88 Welche konkurrierenden Berechtigungen sind administriert?

Zeigt eine Liste der konkurrierenden Berechtigungen an. Konkurrierende Berechtigungen wirken sich nur auf Berechtigungen aus, die das Attribut Ändern gesetzt haben.

Der Berechtigungs-Filter wirkt auf die führende Berechtigung.

#89 Welche konkurrierenden Ber. wurden hinzugefügt oder entfernt?

Zeigt eine Liste hinzugefügter und entzogener konkurrierenden Berechtigungen in einem bestimmbaren Zeitraum an. Konkurrierende Berechtigungen wirken sich nur auf Berechtigungen aus, die das Attribut Ändern gesetzt haben.

#91 Welche Kompetenzen / Eigenschaften haben wie viele MA?

Der Report zeigt gruppiert nach der Anzahl der Bediener beim 4-Augen-Prinzip an, wie häufig Unter- und Obergrenzen von Kompetenzen vergeben wurden. Es werden ausschließlich Kompetenzen von Planstellen mit Mitarbeitern berücksichtigt. Negierte Berechtigungen werden nicht angezeigt!

Wenn beispielsweise für die Berechtigung INL-LASTSCH in unterschiedlichen AZs Kompetenzen vergeben wurden, so zeigt dieser Report dann die Unter- und Obergrenzen der Kompetenzen in den einzelnen AZs an.

#92 Welches Profil vererbt sich an wie viele MA über welchen Berechtigungsträger?

Der Report zeigt die Summen aller Zuweisungen bestimmter Profile zu einem Zeitpunkt an User an, die einer Person, einer Stelle oder einer OE direkt oder indirekt zugewiesen wurde. Bei OE und Stelle wird immer die Useranzahl ausgegeben, die über eine OE oder eine Stelle ein Profil erhält.

Hinweis: Es werden nur solche Oes und Stellen berücksichtigt, denen auch User über die eingestellte Zuordnungsart zugewiesen sind. Wenn z.B. in den Stellen einer OE keine User zugewiesen ist, wird die OE nicht aufgeführt.

#93 Wie viele und welche Profile erhält ein Berechtigungsträger?

Der Report zeigt die Berechtigungsträger mit ihren Profilen, gruppiert nach Berechtigungsart, an. Es wird die Anzahl der Profilzuweisungen gezählt, erhalten mehrere User über eine OE oder Stelle das gleiche Profil, so wird das Profil nur ein mal gezählt.

Hinweis: Es werden nur solche Oes und Stellen berücksichtigt, denen auch User über die eingestellte Zuordnungsart zugewiesen sind. Wenn z.B. in den Stellen einer OE keine User zugewiesen ist, wird die OE nicht aufgeführt.

#94 Welche MA haben vollumfängliche Rechte für Genehmigungen?

Der Report zeigt alle User an, die für das Gesamthaus (OE 0000000 bis 9999999) alle Tätigkeits-ID (00000 bis 99999) Genehmigungen von Berechtigungsvorgängen durchführen können (Berechtigung: KURS_GENEHM). Über den OE-Stellen-Zuordnungsart kann festgelegt werden, welche Zuordnungsarten angezeigt werden.

#98 Welche Berechtigungen haben User einer OE

Der Report zeigt die Berechtigungen, Feindefinitionen und Eigenschaften / Kompetenzen der User einer OE inklusive ihrer Stellen an. Dabei werden solche User zusammengefasst dargestellt, deren Berechtigungen identisch sind, unabhängig davon, über welchen Ursprung die User die Berechtigung erhalten (z.B. über eine OE, eine Stelle oder ein Profil). Wenn keine Attribute setzbar sind und Negiert auf N steht werden die Attribute nicht mit ausgegeben.

ACHTUNG: Bitte prüfen Sie vor Ausführung die Zuordnungsart (HIER_TÄTIG, PLANSTELLE etc.)!!!

Sie können diesen Report verwenden, um einzelne OEs bezüglich der aktuellen Rechtevergabe zu validieren bzw. die Rezertifizierung im Sinne der MaRisk durchzuführen. Durch die "komprimierte" Anzeige (gleiche Berechtigungen aller

Berechtigungsreports / Prüfungsfragen

Bereich Berechtigungen

#98 Welche Berechtigungen haben User einer OE

User einer OE werden voran gestellt) wird der Abstimmaufwand reduziert. Ferner können Sie sich durch die Zusammenfassung der User in Gruppen einen Überblick darüber verschaffen, welche User ein gleichartiges Kompetenz- und Rechtegfüge aufweisen.

Sollten User mit gleichen Funktionen / Stellenbeschreibungen in unterschiedlichen Gruppen erscheinen, so wäre zu prüfen, warum und wie sich diese User von den Usern der anderen Gruppe unterscheiden und ob dies sachgerecht ist.

Der Report berücksichtigt die die Berechtigungskategorisierung des R4Plus, vorausgesetzt diese wurde importiert. Dies gibt Ihnen die Möglichkeit, den Report auf risikorelevante Berechtigungen zu reduzieren.

ACHTUNG: Im Normalfall können Sie das Instituts-Profil hier ausschließen! Bitte wählen Sie im Reiter KURS-Details die für Sie relevanten Berechtigungsträger aus.

#100 Wie viele Mitarbeiter haben welche Berechtigungen?

Der Report zeigt die zu einem bestimmten Zeitpunkt vergebenen Berechtigungen mit der Anzahl der Mitarbeiter, die diese Berechtigungen besitzen, an. "Geerbte" Berechtigungen (z.B. von Stellen) werden hier mit berücksichtigt. Ferner zeigt der Report die Anzahl der Mitarbeiter differenziert nach dem Attribut "Negiert" an.

Falls der R4Plus-Rahmen importiert wurde werden die R4Plus-Informationen mit ausgegeben.

Sie können in diesem Report auch nach User-Typen filtern, sodass Sie gezielt auch technische User abfragen können. Bitte beachten Sie, dass nur User angezeigt werden, die auch per Zuordnungsart Stellen zugeordnet sind.

#101 Welche Berechtigungen werden nicht in der Sparkasse verwendet?

Der Report zeigt alle in OPS sichtbaren Berechtigungen an, die zum gewählten Zeitpunkt NICHT verwendet werden. Berechtigungen an Stellenfunktionen bzw. Funktionsprofilen werden ausgenommen, d.h. wenn Berechtigungen ausschließlich Stellenfunktionen bzw. Funktionsprofilen zugewiesen sind, gelten diese als "nicht verwendet".

#102 Welche User haben gleiche Berechtigungen über OE-Grenzen hinaus?

Der Report zeigt die Berechtigungen, Feindefinitionen und Eigenschaften / Kompetenzen der User mehrerer OEs inklusive ihrer Stellen an. Dabei werden solche User zusammengefasst dargestellt, deren Berechtigungen identisch sind, unabhängig davon, über welchen Ursprung die User die Berechtigung erhalten (z.B. über eine OE, eine Stelle oder ein Profil). Wenn keine Attribute setzbar sind und Negiert auf N steht werden die Attribute nicht mit ausgegeben.

ACHTUNG: Bitte prüfen Sie vor Ausführung die Zuordnungsart (HIER_TÄTIG, PLANSTELLE etc.)!!!

Sie können diesen Report verwenden, um mehrere OEs bezüglich der aktuellen Rechtevergabe zu validieren (z.B. mehrere Markt-Oes) bzw. die Rezertifizierung im Sinne der MaRisk durchzuführen. Durch die "komprimierte" Anzeige (gleiche Berechtigungen aller User einer OE werden voran gestellt) wird der Abstimmaufwand reduziert. Ferner können Sie sich durch die Zusammenfassung der User in Gruppen einen Überblick darüber verschaffen, welche User ein gleichartiges Kompetenz- und Rechtegfüge aufweisen.

Sollten User mit gleichen Funktionen / Stellenbeschreibungen in unterschiedlichen Gruppen erscheinen, so wäre zu prüfen, warum und wie sich diese User von den Usern der anderen Gruppe unterscheiden und ob dies sachgerecht ist.

Der Report berücksichtigt die die Berechtigungskategorisierung des R4Plus, vorausgesetzt diese wurde importiert. Dies gibt Ihnen die Möglichkeit, den Report auf risikorelevante Berechtigungen zu reduzieren.

ACHTUNG: Im Normalfall können Sie das Instituts-Profil hier ausschließen! Bitte wählen Sie im Reiter KURS-Details die für Sie relevanten Berechtigungsträger aus.

#103 Welche techn. User haben welches Änderungsvorgangsprüfkennzeichen?

Der Report zeigt die technischen User an.

Das Merkmal "Änderungsvorgänge in der Änderungs-DB prüffrei stellen bzw. im Kontrollradar berücksichtigen" kann folgende Werte haben:
norm-mKR = normale Prüfung, mit Kontrollradar
prüffrei-oKR = prüffrei, ohne Kontrollradar
prüffrei-mKR = prüffrei, mit Kontrollradar
norm-oKR = normale Prüfung, ohne Kontrollradar

Berechtigungsreports / Prüfungsfragen

Bereich Berechtigungen

#103 Welche techn. User haben welches Änderungsvorgangsprüfkennzeichen?

#104 Welche Stelle hat welche Profile, Funktionsprofile und dir. zug. Berechtigungen

Der Report zeigt alle Profile, Funktionsprofile und direkt zugewiesenen Berechtigungen der Stellen (Soll und Ist) und Usern (Ist der PLANSTELLE) der selektierten Orgeinheiten an. Es werden nur Stellen angezeigt, denen auch Profile oder Berechtigungen zugewiesen wurden.

#105 Welche Stellenfunktionen wurden keiner Stelle zugewiesen?

Der Report zeigt alle Stellenfunktionen an, die keiner Stelle zugewiesen sind.

#106 Welche Stellenfunktionen haben keine Inhalte?

Der Report zeigt alle Stellenfunktionen an, die keine zugewiesenen Berechtigungen oder Profile haben.

#107 Welche Funktionsprofile haben keine Berechtigungen?

Der Report zeigt alle Funktionsprofile an, denen überhaupt keine Berechtigungen zugeordnet sind.

#108 Welche Funktionsprofile wurden nirgends zugewiesen?

Der Report zeigt Funktionsprofile an, die aktuell nicht verwendet werden.

#109 Welche Unterschiede gibt es zwischen Soll und Ist?

Vergleicht das SOLL einer Stelle mit dem IST. Hierbei werden die Berechtigungen des Mitarbeiters, der eine Planstelle besetzt, mit den Soll-Werten der Stellenfunktion verglichen.

#110 Welche Soll-Berechtigungen haben User einer OE?

Der Report zeigt die Soll-Berechtigungen, -Feindefinitionen und -Eigenschaften / -Kompetenzen der User einer OE inklusive ihrer Stellen an. Dabei werden solche User zusammengefasst dargestellt, deren Soll-Berechtigungen identisch sind. Wenn keine Attribute setzbar sind und Negiert auf N steht werden die Attribute nicht mit ausgegeben.

ACHTUNG: Bitte prüfen Sie vor Ausführung die Zuordnungsart (HIER_TÄTIG, PLANSTELLE etc.)!!!

Sie können diesen Report verwenden, um einzelne OEs bezüglich der aktuellen Soll-Rechtevergabe zu validieren bzw. die Rezertifizierung im Sinne der MaRisk durchzuführen. Durch die "komprimierte" Anzeige (gleiche Berechtigungen aller User einer OE werden voran gestellt) wird der Abstimmaufwand reduziert. Ferner können Sie sich durch die Zusammenfassung der User in Gruppen einen Überblick darüber verschaffen, welche User ein gleichartiges Kompetenz- und Rechtegfüge aufweisen. Der Report lässt sich sehr gut mit Report #109 kombinieren: Nutzen Sie 110 um das Soll zu rezertifiziereund und 109 um dann den Soll-Ist-Abgleich durchzuführen.

Sollten User mit gleichen Funktionen / Stellenbeschreibungen in unterschiedlichen Gruppen erscheinen, so wäre zu prüfen, warum und wie sich diese User von den Usern der anderen Gruppe unterscheiden und ob dies sachgerecht ist.

Der Report berücksichtigt die die Berechtigungskategorisierung des R4Plus, vorausgesetzt diese wurde importiert. Dies gibt Ihnen die Möglichkeit, den Report auf risikorelevante Berechtigungen zu reduzieren.

#111 Welche User haben gleiche Soll-Berechtigungen über OE-Grenzen hinaus?

Der Report zeigt die Soll-Berechtigungen, Feindefinitionen und Eigenschaften / Kompetenzen der User mehrerer OEs inklusive ihrer Stellen an. Dabei werden solche User zusammengefasst dargestellt, deren Soll-Berechtigungen identisch sind. Wenn keine Attribute setzbar sind und Negiert auf N steht, werden die Attribute nicht mit ausgegeben.

ACHTUNG: Bitte prüfen Sie vor Ausführung die Zuordnungsart (HIER_TÄTIG, PLANSTELLE etc.)!!!

Sie können diesen Report verwenden, um mehrere OEs bezüglich der aktuellen Rechtevergabe zu validieren (z.B. mehrere Markt-Oes) bzw. die Rezertifizierung im Sinne der MaRisk durchzuführen. Durch die "komprimierte" Anzeige (gleiche Soll-Berechtigungen aller User einer OE werden voran gestellt) wird der Abstimmaufwand reduziert. Ferner können Sie sich durch die Zusammenfassung der User in Gruppen einen Überblick darüber verschaffen, welche User ein gleichartiges Kompetenz- und Rechtegfüge aufweisen. Der Report lässt sich sehr gut mit Report #109 kombinieren: Nutzen Sie 110 um das Soll zu rezertifiziereund und 109 um dann den Soll-Ist-Abgleich durchzuführen.

Sollten User mit gleichen Funktionen / Stellenbeschreibungen in unterschiedlichen Gruppen erscheinen, so wäre zu prüfen, warum und wie sich diese User von den Usern der anderen Gruppe unterscheiden und ob dies sachgerecht ist.

Berechtigungsreports / Prüfungsfragen

Bereich Berechtigungen

#111 Welche User haben gleiche Soll-Berechtigungen über OE-Grenzen hinaus?

Der Report berücksichtigt die die Berechtigungskategorisierung des R4Plus, vorausgesetzt diese wurde importiert. Dies gibt Ihnen die Möglichkeit, den Report auf risikorelevante Soll-Berechtigungen zu reduzieren.

#117 Welche Kritikalitäten gibt es bei Berechtigungen? (Neu)

Der Report zeigt die in OSP erfasste Kritikalität und die hinterlegte R4-Plus-Einschätzung von Berechtigungen an. Es werden nur solche Berechtigungen angezeigt, die im Downloadzeitreim verwendet wurden.

#119 Welche Funktionsprofile u. Berechtigungen sind welchen Stellenfunktionen zugew.? (Neu)

Der Report zeigt alle Stellen / Stellenfunktionen und deren Funktionsprofile / Berechtigungen an Stellenfunktionen der selektierten Orgeinheiten an. Es werden nur Stellen angezeigt, denen auch Funktionsprofile oder Soll-Berechtigungen zugewiesen wurden.

#120 Welche Rollen gibt es pro Stellenfunktion? (Neu)

Der Report zeigt alle Rollen der Mitarbeiter sowie die Stellenfunktion der Stelle an.

#121 Bei welchen Berechtigungen wurde die Kritikalität nicht bewertet? (Neu)

Der Report zeigt die Berchetigungen an, für die in OSP keine Kritikalität erfasst wurde. Ergänzend werden die R4Plus-Risikoeinschätzungen ausgegeben. Es werden nur solche Berechtigungen angezeigt, die im Downloadzeitreim verwendet wurden.

#123 Welche Funktionsprofile werden vom wem verantwortet? (Neu)

Der Report zeigt alle Funktionsprofile sowie deren Verantwortliche an.

#124 Wer verantwortet welche Funktionsprofile? (Neu)

Der Report zeigt nach Funktionsprofilverantwortlichen sortiert die zugewiesenen Funktionsprofile an.

#125 Welche Funktionsprofile haben keine Verantwortlichen? (Neu)

Der Report zeigt Funktionsprofile an, bei denen kein Verantwortlicher hinterlegt ist.

#126 Wie sind die Funktionsprofile ausgestaltet? (Neu)

Der Report erzeugt eine Übersicht aller Funktionsprofile und den darin enthaltenen Berechtigungen inkl. Kompetenzen, sortiert nach dem Funktionsprofilverantwortlichen.

#127 Wer verantwortet folgende Stellen / Funktionsprof. / Berecht. an Stellenfunkt.? (Neu)

Der Report zeigt alle Profile, Funktionsprofile und direkt zugewiesenen Berechtigungen der Stellen (Soll und Ist) und User (Ist der PLANSTELLE) der selektierten Orgeinheiten an. Es werden nur Stellen angezeigt, denen auch Profile oder Berechtigungen zugewiesen wurden. Die Sortierung erfolgt nach Stellenfunktionsverantwortlichen.

#251 Welche KURS-User haben keinen AD-User?

Zeigt KURS-User an, die keinen AD-User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das AD-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!

#255 Welche KURS-User haben keinen WinNT-User?

Zeigt KURS-User an, die in WinNT keinen User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das WinNT-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!

Berechtigungsreports / Prüfungsfragen

Bereich Profil-/Berechtigungsgr.

#13 Welche Profilgruppen gibt es in einer OE?

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter inklusive Feindefinitionen und Eigenschaften / Kompetenzen an. Pro Mitarbeiter werden alle Berechtigungen dargestellt, die sich für Stellen, auf der sich der Mitarbeiter anmelden kann, ergeben.

Technischer User RZ erben keine Berechtigungen des Instituts oder von Stellen / OEs.

Hinweis: Der Report zeigt administrierte konkurrierende Berechtigungen farbig an, wenn sowohl die führende Berechtigung als auch die abhängige konkurrierende Berechtigung nicht durch Filterung im Report ausgeschlossen wurden.

#14 Welche Profilgruppen gibt es?

Der Report zeigt alle Berechtigungen einzelner Mitarbeiter, bei denen Feindefinitionen zugewiesen sind, an und zwar nach Feindefinitionen sortiert. Zusätzlich werden pro Mitarbeiter die Feindefinitionen / Berechtigungen dargestellt, die sich für Stellen, auf der sich der Mitarbeiter anmelden kann, ergeben.

#47 Woher erhalten User in best. Profilgruppen ihre Berechtigungen?

Profilgruppen gibt es in OSP selbst nicht. Eine Profilgruppe stellt die Summe aller Profile dar, die einem Mitarbeiter zugewiesen sind. Sollte ein anderer Mitarbeiter die gleichen Profile besitzen, so gehört er zur gleichen Profilgruppe.

Im Report werden die Profilgruppen, die darin enthaltenen Profile und die Mitarbeiter angezeigt. Direkt Personen zugewiesene Berechtigungen werden hier nicht berücksichtigt. Zusätzlich wird angezeigt, woher die Mitarbeiter ein bestimmtes Profil erhalten haben (über OE, Stelle oder direkt zugewiesen).

Der Report wertet alle Profile aus, auch solche, die an der Stelle oder an der OE hängen aus. Da der Mitarbeiter an einem Tag auf mehreren Stellen zugeordnet sein (wenn er z.B. den Platz wechselt wie bei Springern), stellt dies nur die Profilgruppen der angegebenen "Sekunde" dar.

#70 Welche Unterschiede gibt es im Detail zwischen den "Gesamtberechtigungen"?

Der Report zeigt die Anzahl der Abweichungen aller Berechtigungsgruppen an.

WICHTIG: Die Berechtigungsgruppen in diesem Report werden dadurch erzeugt, dass alle Berechtigungen eines Mitarbeiters inkl. Attributen, Feindefinitionen und Eigenschaften / Kompetenzen mit denen der anderen Mitarbeiter verglichen werden.

Es wird wie folgt verglichen:

In der Berechtigungsgruppe wird nach gleichen Berechtigungen gesucht.
1. Wenn eine Berechtigung nicht vorhanden ist, gilt dies als 1 Unterschied. Es wird nicht weiter geprüft, ob noch Eigenschaften/Kompetenzen oder Feindefinitionen vorhanden sind!
2. Wenn die Berechtigungen gleich sind wird zuerst geprüft, ob ein oder mehr Attribute unterschiedlich sind. Wenn ein oder mehr Attribute unterschiedlich sind, gilt dies als 1 Unterschied (auch wenn mehrere unterschiedlich sind!). Nach der Attributsprüfung wird weiter geprüft.
3. Wenn ein Feindefinitionssatz (FDef1, FDef2 und FDef3 einer Berechtigung) abweicht bzw. in der anderen Profilgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Liegen mehrere Feindefinitionssätze vor, so wird jeder geprüft. Ein Feindefinitionssatz gilt dann als identisch, wenn alle Feindefinitionen inkl. Attribute identisch sind. Nach der Feindefinitionsprüfung wird weiter geprüft.
4. Wenn eine Eigenschaft/Kompetenz abweicht bzw. in der anderen Berechtigungsgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Eine Eigenschaft gilt dann als identisch, wenn die Untergrenzen/Obergrenzen, die Kompetenzausübung im 4-Augen-Prinzip und das Ein-/Ausschluss-Kennzeichen identisch sind.

#71 Wie unterscheidet sich die "Gesamtberechtigung" bestimmter User?

Der Report zeigt die Anzahl der Abweichungen aller Berechtigungsgruppen inkl. Mitarbeiter an.

WICHTIG: Die Berechtigungsgruppen in diesem Report werden dadurch erzeugt, dass alle Berechtigungen eines Mitarbeiters inkl. Attributen, Feindefinitionen und Eigenschaften / Kompetenzen mit denen der anderen Mitarbeiter verglichen werden.

Es wird wie folgt verglichen:

In der Berechtigungsgruppe wird nach gleichen Berechtigungen gesucht.

Berechtigungsreports / Prüfungsfragen

Bereich Profil-/Berechtigungsgr.

#71 Wie unterscheidet sich die "Gesamtberechtigung" bestimmter User?

1. Wenn eine Berechtigung nicht vorhanden ist, gilt dies als 1 Unterschied. Es wird nicht weiter geprüft, ob noch Eigenschaften/Kompetenzen oder Feindefinitionen vorhanden sind!
2. Wenn die Berechtigungen gleich sind wird zuerst geprüft, ob ein oder mehr Attribute unterschiedlich sind. Wenn ein oder mehr Attribute unterschiedlich sind, gilt dies als 1 Unterschied (auch wenn mehrere unterschiedlich sind!). Nach der Attributsprüfung wird weiter geprüft.
3. Wenn ein Feindefinitionssatz (FDef1, FDef2 und FDef3 einer Berechtigung) abweicht bzw. in der anderen Profilgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Liegen mehrere Feindefinitionssätze vor, so wird jeder geprüft. Ein Feindefinitionssatz gilt dann als identisch, wenn alle Feindefinitionen inkl. Attribute identisch sind. Nach der Feindefinitionsprüfung wird weiter geprüft.
4. Wenn eine Eigenschaft/Kompetenz abweicht bzw. in der anderen Berechtigungsgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Eine Eigenschaft gilt dann als identisch, wenn die Untergrenzen/Obergrenzen, die Kompetenzausübung im 4-Augen-Prinzip und das Ein-/Ausschluss-Kennzeichen identisch sind.

#72 Wie unterscheidet sich die "Gesamtberechtigung" verschiedener Stellen?

Der Report zeigt die Anzahl der Abweichungen aller Berechtigungsgruppen an.

WICHTIG: Die Berechtigungsgruppen in diesem Report werden dadurch erzeugt, dass alle Berechtigungen von Stellen inkl. Attributen, Feindefinitionen und Eigenschaften / Kompetenzen mit denen der anderen Stellen verglichen werden. Hierbei ist irrelevant, ob die Stelle von Mitarbeitern besetzt ist.

Es wird wie folgt verglichen:

In der Berechtigungsgruppe wird nach gleichen Berechtigungen gesucht.
1. Wenn eine Berechtigung nicht vorhanden ist, gilt dies als 1 Unterschied. Es wird nicht weiter geprüft, ob noch Eigenschaften/Kompetenzen oder Feindefinitionen vorhanden sind!
2. Wenn die Berechtigungen gleich sind wird zuerst geprüft, ob ein oder mehr Attribute unterschiedlich sind. Wenn ein oder mehr Attribute unterschiedlich sind, gilt dies als 1 Unterschied (auch wenn mehrere unterschiedlich sind!). Nach der Attributsprüfung wird weiter geprüft.
3. Wenn ein Feindefinitionssatz (FDef1, FDef2 und FDef3 einer Berechtigung) abweicht bzw. in der anderen Profilgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Liegen mehrere Feindefinitionssätze vor, so wird jeder geprüft. Ein Feindefinitionssatz gilt dann als identisch, wenn alle Feindefinitionen inkl. Attribute identisch sind. Nach der Feindefinitionsprüfung wird weiter geprüft.
4. Wenn eine Eigenschaft/Kompetenz abweicht bzw. in der anderen Berechtigungsgruppe für diese Berechtigung nicht enthalten ist, gilt dies als 1 Unterschied. Eine Eigenschaft gilt dann als identisch, wenn die Untergrenzen/Obergrenzen, die Kompetenzausübung im 4-Augen-Prinzip und das Ein-/Ausschluss-Kennzeichen identisch sind.

Berechtigungsreports / Prüfungsfragen

Bereich RACF

#62 Welcher User hat sich wann zuletzt am System angemeldet?

Zeigt die existenten RACF-User inkl. Parametern sortiert nach letztem Anmeldedatum (vom ältesten zum jüngsten) an.

HINWEIS: Es werden ausschließlich diejenigen User angezeigt, welche sich im Auswertungszeitraum zumindest einmal angemeldet haben. Ferner führt eine Anmeldung im Portal NICHT zu einem Anmelde-Änderungsdatum in RACF, da durch das Portal "nur" ein Schnellcheck durchgeführt wird.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

#63 Welche User sind in RACF gesperrt?

Zeigt gesperrte RACF-User inkl. Parametern an.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

#64 Welche User haben ein Passwortintervall größer gleich X Tagen?

Zeigt alle User an, bei denen das Passwortintervall größer gleich X Tage ist.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

#65 Welche User müssen ihr Passwort nie wechseln?

Zeig alle User an, die keinen Passwortwechsel durchführen müssen (Passwortintervall = 0).

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

#66 Welche User haben eine RACF-ID aber keine KURS-ID?

Zeigt alle User an, die in RACF eine User-ID haben, nicht aber in KURS

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

#67 Welche User haben eine KURS-ID aber keine RACF-ID?

Zeigt alle User an, die in KURS eine User-ID haben, nicht aber in RACF

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

#77 Welche RACF-Passwortwechsel sind älter als X Tage?

Zeigt alle User mit Kennungen SXXX#### an, die vor mehr als X Tagen zum letzten Mal das Passwort gewechselt haben. XXX ist hier die Institutsnummer, #### die User-ID des Users. Beispiel: S9991234. Es werden auch User mit Buchstaben in den letzten 4 Zeichen der Kennung berücksichtigt (Beispiel: S999ABCD)

User mit Passwortintervall 0 und User, die innerhalb des angegebenen Zeitraums angelegt wurden, werden nicht angezeigt.

Bitte bedenken Sie, dass die FI die Tabellen in der IIB nur Samstags aktualisiert.

#205 Welcher RACF-PW-Wechsel ist jünger als die letzte Anmeldung am AD?

Der Report zeigt alle User an, deren Passwortwechsel in RACF jünger als die letzte Anmeldung in Windows (AD) ist. Die letzte Anmeldung im AD wird aus dem jüngeren Datum der AD-Variablen lastLogon und lastLogonTimestamp gebildet. Der Download der Daten aus RACF und AD muss vom gleichen Tag sein, sonst kann der Report nicht ausgeführt werden.

WICHTIG: Es werden nur Anmeldungen betrachtet, die Älter als 14 Tage sind, da das AD-Attribut lastLogonTimestamp erst nach 14 Tagen auch definitiv zwischen den Domänen-Controllern repliziert wurde. Ferner werden RACF-Daten derzeit nur Samstags in der IIB aktualisiert.

Erläuterung: lastLogon und lastLogonTimestamp unterscheiden sich dadurch, dass lastLogon nicht zwischen den Domänencontrollern repliziert wird, lastLogonTimestamp schon (allerdings erst nach 9-14 Tagen). Der jüngere Werte ist also der "richtigere", wobei der genaue Wert der letzten Anmeldung in der Domäne tatsächlich erst nach 9-14 Tagen im AD über die Variable lastLogonTimestamp ausgelesen werden kann.

Berechtigungsreports / Prüfungsfragen

Bereich Sonstiges

#18 Welche User-Ids weichen von der normalen Syntax ab?

Der Report zeigt alle User-IDs an, die vom Standard abweichen. Im Normalfall steht vor einer User-Kennung ein S und die dreistellige Institutsnummer. Dieser Report zeigt alle Kennungen an, die von diesem Standard, aus welchen Gründen auch immer, abweichen. Er kann somit der Qualitätssicherungen der S-Kennungen und technischer User dienen.

Ab Release 9.0: Der User "Technischer RACF-User" (PNR: 9999001001) wird bei diesem Report nicht angezeigt, da er nur als "Pseudouser" die Unterschiede zwischen RACF und KURS abbildet.

#19 Welche Berechtigungen gab es an einem bestimmten Tag in OSP?

Der Report zeigt alle in OSP vorhandenen Berechtigungen zu einem bestimmten Tag an. Zum Report-Tag nicht mehr gültige Berechtigungen sind gesondert gekennzeichnet.

#25 Welche Berechtigungen wurden in einem best. Zeitraum zu OSP hinzugefügt?

Der Report zeigt die Berechtigungen an, die von der SI in einem bestimmten Zeitraum neu zu OSP hinzugefügt wurden (Schlüsselverzeichnis PRI).

#116 Wer verantwortet was? (Neu)

Der Report zeigt Beziehungen zwischen Objekten in OSP an, z.B. wer verantwortlich ist für bestimmte Berechtigungen oder auch Anwendungen.

#122 Welche Anwendungen haben keine / eine unzureichende Schutzbedarfseinstufung (Neu)

Der Report zeigt Anwendung an, für die keine Schutzbedarfskategorisierung vorgenommen wurde.

Berechtigungsreports / Prüfungsfragen

Bereich Stellen / Rollen

#1 Welcher Mitarbeiter kann sich nicht anmelden?

Der Report zeigt alle Mitarbeiter an, die zum Auswertungszeitpunkt keiner OE zugewiesen sind.

#20 Wer hat Vertretungsfunktionen für einen Stellenwechsel (Ma vertritt)?

Der Report zeigt alle Mitarbeiter an, die die Rolle „MA vertritt“ auf Beraterplätze zugewiesen bekommen haben.

#21 Welcher Mitarbeiter hat welche Rollen?

Der Report zeigt alle Rollen der Mitarbeiter bestimmter OEs an. (hier tätig, Planstelle, MA vertritt).

#22 Welche Stellen sind bei einer OE unbesetzt?

Der Report zeigt alle Stellen einer OE an, die unbesetzt sind.

#24 Wer war wann wo tätig?

Der Report zeigt an, wann bestimme Mitarbeiter welche Stelle besetzt haben (HIER_TÄTIG).

#80 Wer vertritt einen Mitarbeiter?

Der Report zeigt die Stellen des Mitarbeiters an, auf denen der Mitarbeiter eine bestimmbare Rolle hat UND für die es Stellvertretungen zu dieser Stelle gibt. Stellen, für die der User eine Rolle hat, für die es aber keine Stellvertretung (MA VERTRITT oder VERTRETUNG) gibt, werden NICHT angezeigt.

Berechtigungsreports / Prüfungsfragen

Bereich User

#40 Welche User wurden neu angelegt / entfernt?

Zeigt alle hinzugefügten und entfernten (abgelaufenen) User in einem bestimmten Zeitraum an. Es wird nach dem Hinzufüge- / Ablaufdatum sortiert, je nachdem, was relevant ist. Wenn ein User im gegebenen Zeitraum hinzugefügt und entfernt wurde, wird er unter dem "Hinzufüge-Datum" aufgeführt.

Es werden auch User aufgeführt, die "umbenannt" oder deaktiviert wurden.

#250 Welche AD-User haben keinen KURS-User?

Zeigt AD-User an, die in KURS keinen User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das AD-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!

#251 Welche KURS-User haben keinen AD-User?

Zeigt KURS-User an, die keinen AD-User haben.

ACHTUNG: Bitte bedenken Sie, dass das KURS-Datum und das AD-Download-Datum voneinander abweichen können! Es kann also durchaus sein, dass Sie unterschiedliche Zeiträume betrachten!