**« Microsoft Azure DevOps (Session2)»**

**معاونت** توسعه و برند

واحد نرم‌افزار



**فهـرســت**

[**Global notification 2**](#_Toc63084383)

[**Extension 2**](#_Toc63084384)

[**Analytics 2**](#_Toc63084385)

[**Agent tools: 2**](#_Toc63084386)

[**Retention 3**](#_Toc63084387)

[**Security 3**](#_Toc63084388)

[**نتیجه 4**](#_Toc63084389)

در این فصل قصد داریم به دسترسی‌های تیم‌های در دواپس بپردازیم.

در ابتدا به این نکته توجه داشته باشید که برای استفاده از تمامی بخش های Azure DevOps در قسمت Collection> Collection Setting> Access level> Default را روی گزینه Vs Enterprise قرار دهید.



Global notification

در این قسمت تعیین می‌کنیم که به ازای اتفاقاتی که در سطوح مختلف رخ می‌دهد، بتوان روی ایمیل Notification دریافت کرد.



Extension

میتوان Extension‌های مختلفی را روی Azure DevOps فعال نمود. باید توجه داشته باشید که از Extension‌های خود Microsoft استفاده نمایید سایر Extension‌ها ممکن است باعث کندی یا لاگین کردن‌های متعدد شوند که روند کار با Azure DevOps را مختل کند.

 Analytics

با فعال شدن آنالیتیکس، میتوان بدون استفاده از SSRS و SSIS انواع گزارشات رو از Azure DevOps دریافت کرد.



Agent tools:

به منظور انجام دادن اتوماتیک کارها از این گزینه استفاده می‌شود. به طور مثال برای ران کردن دستی تست‌ها از Agent tools استفاده می‌شود.



Retention

حجم ماندگاری دیتا بیس Azure DevOps با استفاده از این گزینه تعیین می‌شود. با استفاده از این گزینه می‌توان دیتاهایی که مورد نیاز نیستند و قدیمی هستند را حذف نمود.

**** Security

در ارئه دسترسی‌ها در Azure DevOps نمیتوان به هر یک از کاربران دسترسی دهیم به دلیل اینکه با کلیک روی نام کاربر انتظار داریم مشخص شود که کاربر چه دسترسی‌هایی دارد بلکه تنها می‌توان مشاهده نمود که در چه تیم‌ها و گروه های امنیتی عضو است بنابراین مدیریت دسترسی‌ها توسط شخص غیر ممکن است و می‌بایست با ایجاد گروه‌های امنیتی و انتساب دادن هر کاربر به آن نقش دسترسی‌ها را کنترل کرد.

ایجاد گروه‌های امنیتی در لایه Collection به عنوان بالاترین لایه، دسترسی های کلانی را ارائه می‌دهد مانند حذف کردن Team Project Collection یاTeam Pproject

برای ایجاد گروه امنیتی در لایه Collection در قسمت Collection Setting در بخش Security روی گزینه New Goup کلیک نمایید و مجوز‌های مورد نیاز با به این گروه امنتی بدهید.

اما برای مدیریت دسترسی ها در سطوح پایین تر می‌بایست گروه های امنیتی را در لایه project‌ها تعریف کرد. در قسمت project setting در بخش security روی گزینه New Group کلیک نمایید و مجوز‌های مورد نیاز با به این گروه امنتی بدهید. سپس اعضای مورد نیاز را در تب Members به این گروه امنتی اضافه کرده و در نهایت گروه امنتی را به Team مربوطه انتساب دهید.

همانطور که می‌دانید، برای هر پروژه Sprint ها و Area های مختلفی می‌توان تعیین نمود؛ شاید نیاز داشته باشد که یک تیم روی Sprint یا Area‌های خاصی دسترسی داشته باشد و اطلاعات مربوطه را مشاهده نماید در این حالت نیز میتوان روی Sprint‌هاو Area ها به گروه های امنیتی مختلف مجوز های مورد نیاز را اعطا کرد. برای این کار در قسمت Project Configuration در بخش مورد نظر (Sprint یا Area) از سه نقطه کنار نام آنها گزینه Security مورد نظر را انتخاب نموده و تیم مورد نظر را انتخاب نمایید.

به طور کلی به منظور ارائه دسترسی به تیم ها به اطلاعات هر sprint یا هر Area دو مورد را بررسی نمایید:

1. تیم را (از قسمت security) به sprint یا Area مورد نظر اضافه کرده باشیم. (به معنی اینکه این تیم روی محصول در حال کار کردن است)
2. به تیم مجوز لازم جهت مشاهده دیتای sprint یا Area را بدهیم.



نتیجه

* برای ارائه دسترسی‌ها بر حسب نیاز از طریق ایجاد گروه‌های امنیتی در لایه collection یا project اقدام شود.
* افراد به گروه های امنیتی اضافه می‌شوند.
* گروه ای امنیتی به تیم ها انتساب داده می‌شوند.
* با استفاده از Area‌ها محصولات شکسته می‌شوند.
* برای ارائه دسترسی به تیم ها به منظور کار روی محصولات، تیم را به Area مورد نظر اضافه می‌کنیم.
* در صورتی که نیاز باشد تیم، به تمامی محصولات مربوط به Area مورد نظر دسترسی داشته باشد تیک فیلد Include Sub Areas را فعال کنید.