**UPS KT from Dublin team part 4 (BCDR)**

October 3, 2022, 10:33AM

35m 5s

 **Dina Helal** started transcription

 **Dina Helal** 0:05  
I started it already.

 **Aravind Siddoju** 0:06  
I have started.

 **Denise Coffey** 0:11  
Perfect. Great. OK. Thank you, Dina.  
I am. OK, So what we're what we're talking about today is the BCD or efforts that are across not just SSD, but it covers WSD and beyond. It impacts other teams.  
And that are contributing to to the servicing of of Windows. So today we're going to just talk about kind of some of the key areas of BCDR and then we can we can have some follow up sessions if needed or we can have will have plenty of time for Q&A towards the end.

 **Halyna Hladkivska** joined the meeting

 **Denise Coffey** 0:47  
So.  
The first thing we want to look at is what is BCDR so business continuity and disaster recovery. So what do we what do? What does it mean to us when we think about BCD or so? It's very much broken into the two components. There's a business continuity component and there's the disaster recovery component. So for business continuity, it's all about the business operations. You can kind of nearly consider the business continuity all about the people side of things when it comes to BCD or.  
So it's about having policies, procedures and documentation in place that mean that if the if there is in our case, in a region that is unavailable, that is second region has the capability from a people perspective to still execute on those required processes that are needed. So you can at a very high level consider the business continuity part, the people side of BCDR.  
And for us, that's all about having Dr DRI capabilities. So it's being able to perform the DRI function, having our TSG's in place, making sure all the documentation is available to support teams, being able to perform the DRI role for our services.  
And the other side of it is around disaster recovery. So this is the deor part and disaster recovery is more the IT or the services side of things. And so this is about how a team will react in the case of a disaster to making sure that services are recovered. So what we're looking at here is about being able to restore service that the you know the impact of loss of data and making sure that the services are running in a healthy state.  
And to be able to enable servicing.  
So that's sort of at a summary level. What we what we think of when we when we consider what BCD or actually is.  
Umm so I wanted to give you an overview of kind of where our journey has been with BCD or it's been going on now like 3 / 3 years for within WSD.  
Umm, you know, busy or is is a continuous journey and you know it's been going on even before 2018. It's not like all of a sudden in 2018 there was a decision that we need BCDR or these these conversations across Microsoft have been going on for many, many years. But just kind of to look back in the last in the last few years just to give you a very high level view of where we have been on our obesity or journey specific within SSD and WSD.  
So in 2018, the Dublin team was set up and the the primary focus of the Dublin team for SSD was as a, you know, the geographical new geographical capability outside of Redmond with the idea that.  
And you know, if there was a natural disaster in the Redmond region that we we had the capability to start doing some parts of our servicing outside of outside of Redmond.  
Umm. And then from, you know, 2018 and 2019 as well, the IDC team came on board primarily around the CFE side of things and obviously that's expanded now with SSD, with RAM and the yourselves with the UPS team. So things have continued to evolve on the IDC front.  
Umm, but what we did around the kind of.  
And in in 2019 time frame, we really started to formalize our goals around BCDR and there was a lot of discussion because when we think about Windows servicing capability, as I said at the beginning, you're not just talking about about ESD or WSD. Teams are friends in the ESS team, the engineering system team, they have a huge part to play, especially from the build side of things and the build infrastructure. They have a huge part to play in enabling our servicing capability.  
And so this is something that we were working on, you know across multiple teams. But what we really started to do in 2019 was to figure out what is our goal, what is it that we're actually trying to do here and bearing in mind that there's.  
There is, yeah, the you could, you know, you could boil the ocean when it comes to thinking about BCDR capabilities. So we had to be very, very specific and targeted in what our goal is so that we could actually kind of define measures and work to, you know, the teams could work towards that goal together. So there was a lot of time spent in that kind of 2019 even into early 2020 where it was a lot of gap analysis and research and conversations and figuring out targets.  
Because if you think of all of the services that are involved and when services I'm talking about service tree, service and services. And if you think of all of the services that are involved in Windows servicing, we had to figure out what were the ones that we were really interested in. So we set our objective to be that we wanted the ability to still keep our customers protected. In the case of.  
8 natural disaster in the Redmond region.  
Umm, so we we were very specific that it was Redmond going offline and that it was a bee week of Patch Tuesday. We weren't looking at other servicing capabilities. That was just to be able to get a B week update out the door to our customers. And it was also not to enable this as a sustained capability because you know then you're looking at a whole other story. If this is something where you want to be able to run service thing without Redmond, you know for a year.  
You know that's a whole different, a different conversation.  
So we very much targeted it to that and within those parameters we then had to do an activity of working with every single team involved in servicing and identifying what are the, what were the services and also what were the processes or you know policies or procedures that were required for us to maintain if Redmond was offline. So we scoped it down. I think at the moment there is about 5050 odd services that are in scope.  
And for our beside your efforts and then obviously there's processes like release management is a massive aspect of our servicing capability, our calms teams with release notes, release notifications and you know, so it does go beyond services, but we you know that was kind of what we had scoped our our project to be.  
Though team set off working towards Umm, working towards achieving those goals and we'll talk more specifically in the next couple of slides about what those what those goals are you know and how we measure BCD or but we were doing that project was kind of ongoing for another year and a half or so and then in 2021.  
Mike Fortune, who's now retired but M14 needs to be Umm Carlos.  
Manager and Mike said, you know, it's all great what we're doing here, at least to do our, but what if we were to do more? What if we were to enable the capability of literally being able to service from any location for any product? Because our original objective was just for Windows 10. So we weren't looking at anything down level. So for any, you know, if there was a natural disaster anywhere, could we just continue to be able to give our customers the same level?  
And of of updates that we give them today. So as you can imagine that's a much, much bigger entity and that's a much a much broader goal. But what we did over the really kind of from the summer of 2021.  
And up through until maybe kind of.  
And before, before Christmas into the autumn, into winter of 2021, and we spent a huge amount of time basically going through the same exercise again, but from a much broader perspective. So looking at what would it take for each team to be able to service from any location for any product for a sustained amount of time so.  
Umm, you know, Mike and Carlos were very clear with us in that if you know, God forbid, there was a natural disaster somewhere, we wouldn't know exactly how long it will take for that location to come back online again. So we can't set a time limit on this. We can't say, OK, we need to be able to manage all the servicing out of IDC for three months. We didn't want to put those constraints of that time frame on it. So what we did was we did a massive big, huge new gap analysis exercise and new funding.  
Exercise.  
And we went through panos reviews. We had reviews with lots of different leadership teams across many, many organizations and divisions. And we came up with this one Microsoft view of what it would take to enable this capability.  
And now, unfortunately, that was also during the times of COVID.  
And we have, you know, a different landscape in the world at the moment. We had, you know, a war started. You know, there's many different things that have impacted and you know, right now where we're in this hiring pause. So the timing was not great in terms of our funding, ask for BCD or so, although we have very senior level support for enabling that capability and the broader BCDR capability, we don't have the finance capability just yet.  
To to proceed with that you were talking.  
You know, you know, for example, I I think it was something like adding another nearly 400 FTE and across the organization. So this was significant.  
Umm, so that funding ask is is on hold for now, but it is definitely something that we will that we will revisit.  
And so the decision that we that we took at the beginning of this calendar year was to revert back to focusing on our original objective, which is the Windows 10 KB capability. If Redmond is offline, that we're able to get a B week update out the door.  
So that's kind of our our journey of where we've been. So you'll hear people talking about like this, you know, new Windows funding requests and everything that that was the big effort that we did last year that's on hold for right now. So just to make sure everyone is on the same page, our BCDR focus right now is for that Windows 10 B week to maintain the capability that teams have enabled so far.  
And to have a quarterly exercises that we do for BCD or to demonstrate our capability and we also have a requirement around there is an S360 requirement for beside or manager compliance and this is a tool where we have to attest or capability and achieve the green light for for BCDR.  
So does anyone have any questions just on on that kind of journey that we've that we've been on so far? I'll, I'll pause there.  
No. OK.  
The we'll move. We'll move on.  
Umm. So just to reiterate our our target is all about well, it's supposed Windows 11 now it's it's about keeping our customers protected and secure. So our focus is on.  
Is on her be week or focus is on security and then we talk about this less than two days of scheduled today. So we have there's lots of different acronyms when it comes to BCD or you have your ortc which is your recovery time capability. And our goal is that we would have no more than two days delay of AB week update that was being sent out to the customers. In the case of a of a of a natural disaster.  
And and on that natural disaster, so just so there's, there's no confusion as well. You're probably you've you've heard of different efforts around the secure supply chain and the executive order and there's a lot of security focus that is going on around that project right now.  
When that's at the there you know the scenarios there are all about like malicious actors coming and deliberately doing something you know to try and and impact our servicing capability or what goes out to her customers. When we talk about our BCDR project, we're talking about a natural disaster. So we're talking about an earthquake, volcanic eruption, something like that. That happens in the Redmond region that would basically like lights out for the Redmond team.  
You know, both in terms of like people not being available lights like literally no lighting, no electricity, no machines available like nothing. So when we're talking about BCDR, it is very much about the natural disaster aspect of things rather than the malicious actor.  
OK, so there are three components of BCDR. So whenever we're talking about a BCDR plan and we always look at it from 3 different aspects, we have our services aspect, our process and people. So service process, people are always the three different aspects that you'll hear me or your BCD or PM champ talking about. So just for that. So Lisa Baldwin is the BCDR PM champ for.  
For UPS, so Lisa, I work with Lisa and she will kind of, you know work with all of you to make sure that as you know as part of your queue two planning if there was anything for BCD or Lisa would be helping to ensure that that is listed in your quarterly plans. So when we think of services, we have a measure called the service maturity model or SMM level. So these are not defined by WSD, these are Microsoft defined.  
Levels and that will go through to now in a minute, but these are, you'll hear talk of SMM level 4 and that is the target for our Windows servicing capability for BCD or we want to make sure that all of our services achieve SMM level 4 SMM level 4 is the Super automated capability, but that is the measure that we use for our services.  
For our processes, it's all about the exercises that we do and the compliance that we have in place. So processes, sorry exercises we previously when we were semester based, we would aim to do an exercise on a semester basis. But as things have matured and as now we've shifted to this quarterly cadence, we are trying to drive a quarterly exercise capability for for bestgore.  
Compliance then comes back to the BCDR manager and this is the S 360 compliance and that we have to have for all of our services.  
And then from a people perspective, it's all well and good having the services ready. But you know we're not, we're not 100% hands free for everything. We have to have people in region, we have to have people outside of Redmond who are capable of doing 2 roles and this is important again where you break it down between disaster recovery and business continuity. So one aspect is having people who can make sure that the services have recovered or that they have failed over or that they have continued to run in a healthy state.  
So that's the the people responsible for making sure that disaster recovery is complete and achieved for those services. And then you have the business continuity aspect of people where you're enabling the capability for once those services are healthy again and we can continue our servicing processing of the servicing model that people are there to be able to perform DRI for the services that are required for servicing at B week.  
Any questions on any of that so far?  
OK, we'll keep going.  
And so when we look at our at our SM level, so this is the service maturity model level and this is specifically tied to services and it's how we measure services. The target for WSD and for Windows servicing capability is that all services achieve SMM level 4.  
Umm. And I'll just kind of talk you through kind of the progression there is some level one, but it basically means you, you OK you have a service but it has no capability whatsoever. But really as we look at SMM level 2 into 3 into 4 right now for SSD and for WSD or services or sitting between the SMB 3 and SMW #4 within WSD, there are a couple of CPC services that are SMM level 2.  
And that's a A signed off risk because those services are on the deprecation path. So you know they're we didn't we made the decision not to continue to invest in the SMM progression of those services because they are being deprecated but basically SMM level 2 is that everything is manual, there's nothing automated and you haven't really like there's a disaster recovery plan or a DRP document. And that document is the steps that an engineer is required to take.  
To perform the disaster recovery role and to verify that the service is in a healthy state and so you know for some level 2 you might have only just created that you may not be in a state where you're able to actually do any exercises. So we would do what are called tabletop conversations where we don't actually execute anything. We talk through the recovery capabilities. So it's very, very and an immature estate from a A.  
Service capability perspective.  
But where we really want people to be, UM is at minimum and SM three. But really SMM four is the target. What SMM 3 gets us is it moves away from a manual capability to a more automated. So it's automated, but there's still an element that, you know, the official definition is automated within one to two commands and. But really what we're saying is that for SMM 3.  
If the you know the hugely important part is that we have a multi region capability, we have the ability that if the primary location goes down that we have a second location that we can recover the service to and it's about being mature at that stage of knowing what the dependencies are because it may be a case that to start your recovery of your service you are dependent on other services to be recovered before you can start. So it's being much more mature in the awareness and.  
And an understanding of what it takes for your service to be to recover and what you know what, maybe for you to be able to verify that your service is up, you have to actually go and wait for another service to be recovered as well before you can validate that yours is up. So you know it's web being very, very clear on what those dependencies are. We would expect at that stage that the disaster recovery plan is validated, which means that you would have actually gone and had.  
An engineer or team of engineers who didn't write the documents. They're not the people who actually wrote the document and go and start from step one, walk through the disaster recovery plan and actually prove that they can recover the service just by following the steps in the document. So it's really important that those documents are created, that somebody, you know it does specify in the document what the skill set is required to be able to recover that service. But you shouldn't have to be.  
Working on that service to be able to follow the instructions and recovers.  
And then we we have a measured ortc or recovery time capability. So this is where we can actually valid by validating that do RP we can also time that so we can see how long it actually takes for us to recover our service.  
And then we've progressed into SM Level 4, where we're talking about everything being automated. So this is our happy place of ideal is you're running in an active active configuration that's not required, but it is, you know that is the ideal state and that everything is automated.  
And we have at that point for SM level 4 uh, we we know the services has you know has hit a bump in the road just had to be recovered and because we are monitoring it we have it an indication of service health. Our requirement here is that all services are monitored by EDEM. So EDAM is a SSDL owned.  
And SSD owned service and that in itself also needs to be BCDR compliant and and that service is is owned by the UPS team here in Dublin and the team here evolved that that service kind of quarter on quarter. But the idea here is that you you will know when you're service is down because EDAM is monitoring it and EDAM is triggering an ICM to tell you that your service is unavailable.  
Umm, when we look at SMM four, it's about reaffirming things. It's about retesting your to your ortc, making sure you know we know we all know that service is evolve, the infrastructure around services evolve. So it's not a case that we can say we attest in 1/4. Yep, we've done our job, we're smooth before we've been tested to this or etc.  
Those services will evolve so you have to continue to attest to it. You have to continue to exercise and you have to continue to update your documentation. Both the disaster recovery plan and the TSGS for the DRI capabilities. So it's not, you know, when you think about BCD or it's not a box that you check and say yes, if achieved a job done, I don't need to do anything more. There's a maintenance required quarter on quarter to maintain that that BCDR capability.  
And so I have a link here in the doc that I'll share to you. This is a link to the much more detailed definition of what the SM progressions are and this link down here to the SharePoint list. This is the list link to see all of the different services that we have defined as in scope that are required to meet this SMM level form. So you can take a look at those offline. As I said, I think there's about 52 possibly services across.  
And the organizations that are required to achieve SMM level 4.  
So that's that's kind of a somewhat detailed view of our SMM progression. And then when we look at our BCDR manager compliance, so this is our process component of BCD or so. This is a link there to the BCDR manager tool and BCDR manager compliance and BCDR manager data. It is driven by service tree.  
So if you have a service and service tree that is either classified as GA or even the ones that are classified as closing down because they're still live, but if they're, if that's what their life cycle is classified as, and if the service itself is classified as either online service infrastructure or platform service, it will then appear in BCDR manager with the requirement for us to attest to BCDR manager compliance.  
And busy door Manager compliance is all about it's really it's it's providing for for visitor manager. It's a 12 monthly compliance cycle. So you have to attest to your capability every 12 months and be sad or manager and what you have to show is 3 screenshots. The first screen shot is of the service running healthy in region A. The second screenshot is showing that the service is unavailable in region A and then the third screenshot is showing that the service is now running held in a healthy state.  
In Region B, so it's basically showing the service is running. We've hit a problem, it's unavailable, but I've recovered it to a second location, so that's the. That's the BCDR manager at a station and that is that is required right now with an SSD, we have 100% compliance doesn't mean that we're like 100% SMM for there's a difference there. Compliance with MVCC or manager is about.  
And.  
Is about transparency of your state. It doesn't mean that you have to meet SM4, but it's just about transparency of the actual state for your obesity or capability. SSD at the moment is 100% compliant across WSD where 80% compliant. So as I said, these are things that will come up on the 360 reports that are highlighted within the leadership team.  
Umm, so that's our visitor manager compliance and.  
Oh, sorry.  
Back.  
And so where we are right now for for SSD and for all of the services in terms of compliance, when I look at here for all of the services, this is for all of the teams involved, this is not just specific to WSD. So this is where we stand right now. You know the ESD and WSD numbers are much better. So we do have some other teams who need to ensure that they that they meet that compliance requirement.  
And and in terms of SMM levels where we stand is for SSD, 50% of our services are listed as SMM 4 and 50% are SMM 3.  
Am I know within the UPS team there's a lot of work happening for on the PM side of things and that PME work is contributing to enabling obesity or capability. So my understanding right now is that the UPS team will continue to invest in the PME efforts through Q2 and possibly into Q3 and there's a tentative target of UPS being able to participate in a beside or exercise.  
For two Co within the Q3 timeframe and but there is a caveat that that is dependent on the progress of the PME effort. So that's my understanding of where things stand right now from a UPS perspective. When we when we look at at BCDR.  
And then just to to to reiterate that this is this is a team effort BCD or for Windows servicing is a mammoth undertaking by many many teams. So we have WSD, we have the engineering systems, team monias, we have peers, asks and the EDS team. So that's sort of like the, you know, our signing for our builds everything and then we have the egg security team. And so there's many, many teams involved. And obviously then within within WSD.  
And we have the the full, Umm, kind of break out of all of the the the WSD teams involved.  
So that kind of brings to it to the end of the the specific content that I that I wanted to share with you today, but we can open for questions or if there's specific areas that you'd like to deep dive in in the future, please just drop me a mail or stick a comment in the chat and we can take a look at it. But if there's any questions we can.  
We can talk through those now.

 **Jelena Maksimenko (CPL Solutions)** 29:45  
Thinking that it's.

 **Denise Coffey** 29:50  
Well, hopefully that was Umm that was somewhat enlightening for you to to get a view of of of BCDR again. I suppose the main things for in terms of what our goals are, it's about that natural disaster enabling the capability for for security updates and in the in the short term.  
And I would say, you know, you know, talk to your your leads within within region about you know questions if you have any questions about kind of specific work that you guys are doing right now or plan to do maybe in the next quarter that are specifically contributing to the BCDR efforts.  
And you know the the PME is a significant part of that. So I've, I've no doubt that everybody at some point will will be working on a on an aspect of of BCD or.  
I'm from UPS perspective. We do, you know within the the Dublin team when we look at the DRI pieces. So that is continued to expand the DRI capability within Dublin. And I'm sure there will be a a DRI capability that gets enabled and you know as the team continues to on board within the the IDC team as well.  
And we do have a.  
And even for the original objective, we know that we have a gap in terms of people to be able to support all the UPS services for DRI. So I don't even think with between Dublin and IDC that there is the full.  
You know the number of people required to be able to do full DRI, but we'd have to look and see kind of where that stands right now and kind of what the the onboarding plans are there.  
OK. If there's no questions, then we can we can finish there and feel free to reach out to me directly. If there's anything that you think of after the after the session that you'd like to ask.  
Umm, but if not, I think we can leave it there.

 **Dina Helal** 32:02  
Thanks, Denise.

 **Bhaskar Verma** 32:02  
We need the English. I have one question.

 **Jelena Maksimenko (CPL Solutions)** 32:03  
Legends things, Denise. Thank you. Thanks. Bye.

 **Yashasvini Rathore** 32:04  
Thank to me. Thank you.

 **Denise Coffey** 32:06  
Yeah, you have a question. Yeah, go ahead.

 **Bhaskar Verma** 32:08  
So what did you mean by your service being in GA?

 **Denise Coffey** 32:15  
Umm, so if a service if in service tree the the service is listed as GA is in general availability that it's a service that's used in in production and then it is considered a ABCD or requirement for for beauty or manager compliance.

 **Bhaskar Verma** 32:32  
Oh, OK.

 **Denise Coffey** 32:32  
So each each service and service tree, UM requires a life cycle.  
Umm, but categorization.  
And within service tree, so the whoever owns that service and service tree will set what that life cycle categorization is.

 **Bhaskar Verma** 32:52  
Because.

 **Denise Coffey** 32:57  
Umm, so I'll, I'll send on a link to the deck and I would say like take a look at BCDR manager. Take a look at the services that are listed. Obviously you know we have our UPS services.  
We have E down. We have one pub next Gen AWE and pub suites. I think they're the main UPS services that are in scope for, for BCD or and.  
I am not going to get this right. I think it's AWE and.  
Is that agwa one pub that are have a lot of PME work going on right now that are not SMM four, I think they're the ones that have to, but I'd have to go to the SharePoint list to know for sure, but I think there's two of the UPS services that are still to achieve SMM level 4 and they're the ones with the primary PME work happening in Q2 and into Q3.  
OK, so if there's nothing else and enjoy the rest of your day. And as I said, I'll send them a link, yeah.

 **Dina Helal** 33:56  
I'm sorry, I'm sorry, unrelated question, but do you guys want to have a session next week? Do you have any specific topics in mind? We were thinking to go over the life cycle of, yes, the release tickets that go through movies, 6 next Gen or if you guys have any other topics we can continue the discussion in the chat if you want to have a session next week?

 **Deepak Kunwar** 34:36  
Yeah. So thanks, Dina. So we can go with it.  
And later on, if we have any more topics then we will let you know.

 **Dina Helal** 34:43  
OK, sounds good. Thanks.

 **Deepak Kunwar** 34:45  
Thanks.

 **Denise Coffey** 34:47  
Perfect. Thanks everyone. Enjoy the rest of your day.

 **Dina Helal** 34:51  
Thank you. Bye.

 **Jelena Maksimenko (CPL Solutions)** 34:52  
Thank you. Thanks mate. Bye.

 **Deepak Kunwar** 34:53  
Thank you everyone.

 **Aravind Siddoju** 34:53  
Thank you. Bye. Thank you. Bye.

 **Denise Coffey** 34:53  
Yeah. Bye. Bye. Thank you.

 **Kush Mishra** 34:55  
I.

 **Denise Coffey** 34:55  
I.

 **Dina Helal** left the meeting

 **Jelena Maksimenko (CPL Solutions)** left the meeting

 **Kush Mishra** left the meeting

 **Denise Coffey** left the meeting

 **Pinar Sen** left the meeting

 **Lacastan Moodley** left the meeting

 **Halyna Hladkivska** left the meeting

 **Bhaskar Verma** left the meeting

 **Yashasvini Rathore** left the meeting

 **Aravind Siddoju** left the meeting

 **Deepak Kunwar** left the meeting

 **Dina Helal** stopped transcription