وزارة الاتصالات والتقانة
MINISTRY OF COMMUNICATION & TECHNOLOGY

مشروع توريد وتركيب وتشغيل منظومة الحوسبة السحابية لمشروع الحكومة الإلكترونية السورية

دفتر الشروط الفنية

1. المحتويات

2. مسرد المفردات

Term in English	الاختصار	التعريف
National Agency for Network Services	NANS	الهيئة الوطنية لخدمات الشبكة، وهي الهيئة
Software Defined Data Center	SDDC	مركز البيانات المعرفة برمجياً
Infrastructure as a Service	IaaS	تقديم البنية التحتية كخدمة
Platform as a Service	PaaS	تقديم المنصة كخدمة
Software as a Service	SaaS	تقديم التطبيقات كخدمة
Anything as a Service	XaaS	تقديم أي إجراء برمجي أو تقني كخدمة
Storage Virtualization		مكون تقديم التخزين بشكل افتراضي
Network and Security Virtualization		مكون إدارة الشبكة والحماية بشكل افتراضي
Compute Virtualization		مكون تقديم المعالجة بشكل افتراضي
System Information and Event Management	SIEM	إدارة معلومات الحماية وأحداث الحماية
Log management		إدارة السجلات
Cluster		بنية عنقودية
Storage Area Network	SAN	وحدات التخزين الشبكية
Compression		ضغط البيانات
Deduplication		إلغاء تكرار البيانات
Fault Tolerance		الحماية الذاتية والتعافي من الأضرار
Thin provisioning		ميزة الاستهلاك على قدر الحاجة
Virtual Machine	VM	مخدم افتراضي

Term in English	الاختصار	التعريف
load balancing		توزيع الأحمال
Simple Network Management Protocol	SNMP	بروتوكول إدارة الشبكة
Role-based access control	RBAC	توزيع الصلاحيات على المستخدمين حسب المهام
Pay as you go		الدفع حسب الاستهلاك
Allocation pool of resources		تخصيص حزم استهلاك
Reservation pool of resources		نظام حجز الموارد المسبقة
Flex allocation model		طريقة تجميع مرنة
What-if Analysis		تحليل سيناريوهات (ماذا – لو)
Workflow engine		مكون الأتمتة
Incident Response		الاستجابة للحوادث
machine learning		تعلم الآلة
Threat Intelligence		تقصي معلومات متعلقة بالتهديدات
Protocol Intelligence		تقصي معلومات متعلقة بالبروتوكولات
User Intelligence		تقصي معلومات متعلقة بالمستخدمين
Web intelligence		تقصي معلومات متعلقة بحركة الوب

3. مقدمة

تمثل هذه الوثيقة الشروط الفنية لتنفيذ مشروع توريد وتركيب وتشغيل منظومة الحوسبة السحابية لمشروع الحكومة الإلكترونية، وتهدف هذه الوثيقة إلى تزويد الجهات العارضة بجميع المعلومات والمتطلبات اللازمة لتقديم العرض الفني لتنفيذ المشروع.

هذه الوثيقة موجهة إلى جميع الشركات العاملة في مجال تقانة المعلومات المحلية التي تحقق الشروط المذكورة في الوثيقة لتقديم العرض المطلوب وتنفيذ متطلبات المشروع.

3.1. معلومات عامة

إن بنية المعالجة السحابية هي حل برمجي متكامل يضمن توافر الموارد المطلوبة لتشغيل وصيانة ومراقبة مراكز بيانات افتراضية من كافة الجوانب التقنية (المعالجة والتشغيل والتخزين والوصل الشبكي والحماية ..... الخ) عند الطلب دون تدخل يدوي من مزود الخدمة، وهو مصطلح يصف مراكز البيانات المتوافرة للمستخدمين عبر الإنترنت؛ وقد تكون مراكز البيانات تلك خاصة بشركة واحدة أو متاحة لعدة شركات /هيئات/ منظمات.

تمكن بنية المعالجة السحابية المشتركين من تجنب التكاليف العالية المنفقة على البنى التحتية والعتاد والتشغيل والصيانة...الخ.

وتؤتمت بنية المعالجة السحابية عملية تقديم الخدمات بسرعة عالية ودقة بأقل التكاليف والجهود، بالإضافة إلى المرونة في التجاوب مع المتغيرات الطارئة على بيئة العمل.

كما تمكن بنية المعالجة السحابية المشتركين من الاستفادة من التقنيات الحديثة دون الحاجة إلى طواقم تقنية خبيرة في طريقة تنفيذ وتركيب هذه التقنيات وبأقل التكاليف.

تكون بنية المعالجة السحابية عادة مقدمة من قبل مزود خدمة معالجة سحابية وفق طريقة ونموذج الدفع على قدر الاستخدام، وبالتالي توفير في المصاريف والتكاليف التشغيلية على المشتركين.

تساعد البنية في إزالة الحواجز الكبيرة التقليدية في مراكز البيانات دامجة تقديم المعالجة والتخزين والموارد الشبكية لتسهيل دعم تنصيب التطبيقات من البداية حتى النهاية.

كما تساعد البنية السحابية مدراء البنية السحابية في تقديم بيئة التطبيق بشكل لحظي بدلاً من إرسال طلبات والانتظار من أجل تقديم التخزين والشبكة.

إن الطريقة الأفضل لتركيب البنية التحتية الخاصة ببنية المعالجة السحابية هي استخدام مراكز البيانات المعرفة برمجياً (SDDC).

3.2. فوائد البنية السحابية

- تحسن أداء المنظومات من حيث توفير المرونة وتلبية متغيرات العمل بسرعة وبجهد وتكلفة أقل.
- تقليل التكاليف والمصاريف حيث يوجد استخدام أمثل للموارد دون هدر من حيث تطبيق نموذج الدفع على قدر الاستهلاك.
- الاستقلالية عن المكان والمعدات المستخدمة للوصول حيث يمكن الوصول إلى الموارد من أي مكان ومن أي جهاز ذكي.
- القيام بعمليات الصيانة دون الحاجة إلى توقف بالإضافة إلى ضمان حماية البيانات من خلال التقنيات الحديثة بسهولة وبطريقة مؤتمتة.
- مراقبة الأداء والجودة بسهولة دون الحاجة إلى فرق احترافية بالإضافة إلى حل المشاكل بسرعة.
- زيادة الإنتاجية من خلال سرعة الوصول والربط بين الهيئات والمنظمات بطريقة أمنة.
- الحماية والأمان لأن البيانات والموارد موجودة في مكان مركزي بالإضافة إلى إمكانية توزيعها إلى عدة مناطق منفصلة جغرافياً.

3.3. الأطراف الرئيسية

فيما يلي قائمة بالأطراف الرئيسية المعنية بهذا المشروع:

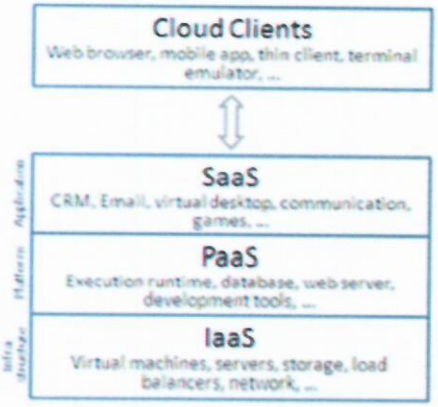
- وزارة الاتصالات والتقانة: مهمتها الإشراف العام على إدارة تطوير المشروع.
- الهيئة الوطنية لخدمات الشبكة: مهمتها تشغيل المشروع واستضافة كافة مكوناته.
- الشركة المنفذة: مهمتها تنفيذ كافة المهام والمتطلبات الواردة في دفتر الشروط الفنية وتقديم الدعم الفني اللازم لعمل المشروع واستثماره بالشكل الأمثل.

4. توصيف الحل

4.1. الرؤية

توريد وتركيب وتشغيل منظومة الحوسبة السحابية لمشروع الحكومة الإلكترونية السورية، لتشكل البنية التحتية لمشروع الحكومة الإلكترونية في الجمهورية العربية السورية، حيث سيتم تشغيل بوابة الحكومة الإلكترونية والناقل الحكومي الإلكتروني الوطني عليها كمنظومات أساسية، وذلك في مركز المعطيات الوطني في الهيئة الوطنية لخدمات الشبكة.

4.2. نماذج خدمات البنية السحابية



1. **IaaS: تقديم البنية كخدمة:**

تقدم للمشتركين/المستخدمين البنى التحتية الأساسية من كافة الجوانب (معالجة / شبكة / تخزين / النسخ الاحتياطي / توزيع الأعمال / ...الخ). هذه البنى التحتية تكون مقدمة بطريقة برمجية مؤتمتة ومركزية وآمنة. ويمتلك الزبون في هذا النموذج كامل الحرية في إدارة البنية المقدمة له، أي يمتلك كل الإمكانيات التي يقدمها مركز البيانات دون الحاجة إلى شرائه واستضافته بشكل فيزيائي وصيانته.

2. **PaaS: تقديم المنصة كخدمة:**

تمكن المستخدمين من تركيب برامجهم وتطبيقاتهم بسهولة وسرعة عن طريق الخدمات والمكتبات البرمجية والبرمجيات والأدوات المقدمة من قبل مزود خدمة المعالجة السحابية من دون الحاجة إلى إدارة البنى التحتية (شبكة التخزين / موارد المعالجة ... الخ).

3. **SaaS: تقديم التطبيقات كخدمة:**

تمكن المستخدمين / المشتركين من استخدام البرمجيات المقدمة من قبل مزود الخدمة دون الحاجة إلى شراء وتركيب وصيانة البنية التحتية المشغلة لهذه البرمجيات والتطبيقات. تعمل معظم تطبيقات SaaS مباشرة على متصفح الإنترنت مما يلغي الحاجة إلى القيام بأي تحميل لأي تطبيق أو تنصيبه على حاسب الزبون مما يلغي الحاجة لوجود فريق IT ليقوم بتنصيب البرامج على كل حاسب بشكل منفصل.

4. **XaaS:**

تمكن المستخدم من استخدام وتنفيذ أي إجراء برمجي أو تقني يريده وفق الإمكانيات المقدمة من مزود الخدمة بطريقة مؤتمتة.

4.3. مكونات البنية السحابية

يتكون القسم البرمجي للمنظومة المراد تنفيذها من الأجزاء الرئيسية التالية:

1. مركز البيانات المعرف بشكل برمجي (Software Defined Data Center): والذي يحوي 4 مكونات رئيسية:
   1) مكون لتقديم التخزين بشكل افتراضي (Storage Virtualization).
   2) مكون لتقديم وإدارة الشبكة وتقديم الحماية بشكل افتراضي (Network and Security Virtualization).
   3) مكون لتقديم المعالجة بشكل افتراضي (Compute Virtualization).
   4) مكون إدارة مركز البيانات المعرف بشكل برمجي
2. مكون لإدارة البنية السحابية: يتألف من عدة مكونات رئيسية:
   1) مكون خاص بالعمليات (operations)
   2) نظام خاص بالأتمتة والتنظيم (Orchestration)
   3) مكون خاص بإدارة الأعمال (Automation)
   4) مكون خاص بإدارة السجلات (Log management)
3. نظام لإدارة معلومات وأحداث الحماية والأمن (SIEM – System Information and Event Management) خاص بالبنية السحابية.

4.4. الإطار

4.4.1. الإطار الزمني

إن الفترة الزمنية المحددة لإنجاز المشروع هي ثمانية عشر شهراً بدءاً من تاريخ المباشرة حتى الاستلام المؤقت، وسنة ميلادية حتى الاستلام النهائي (فترة ضمان مجانية). على أن تكون المدة الإجمالية للمراحل الثلاثة الأولى /ستة أشهر/، و/اثنا عشر شهراً/ للمرحلة الرابعة وعلى العارض تقديم وثيقة برنامج العمل لتنفيذ المشروع ضمن الفترة الزمنية المحددة متضمنة مدد التوريد والتركيب والتنفيذ البرمجي والتشغيل والتدريب للمراحل الآتية:

1. المرحلة الأولى: توريد التجهيزات العتادية، تبدأ من تاريخ المباشرة.
2. المرحلة الثانية: تركيب التجهيزات وتنفيذ مركز البيانات المعرف بشكل برمجي (SDDC): تبدأ بعد استلام مخرجات المرحلة الأولى، وتشمل:
   1. تركيب التجهيزات في بيئة الاستضافة في مركز المعطيات الوطني في الهيئة.
   2. تنفيذ مركز البيانات المعرف بشكل برمجي.
3. المرحلة الثالثة: تنفيذ مكون إدارة البنية السحابية ونظام إدارة المعلومات وأحداث الحماية والأمن، تبدأ بعد استلام نتائج المرحلة الثانية أو يمكن تنفيذها على التوازي مع المرحلة الثانية.

4. المرحلة الرابعة: التشغيل والتدريب، تبدأ بعد استلام أعمال المرحلة الثالثة، ومدتها اثنا عشر شهراً، وتشمل:
   1. تدريب العاملين في الوزارة والهيئة على إدارة وتشغيل المنظومة (يحدد العدد والخبرات المطلوبة لاحقاً).
   2. تشغيل المنظومة لمدة سنة ميلادية كاملة وفق اتفاقية مستوى خدمة توقع مع المتعهد قبل بدء مرحلة التشغيل.

   ملاحظة: يتم الاستلام المؤقت للمشروع في نهاية هذه المرحلة.

4.4.2. الإطار الفني

يجب أن تحقق المنظومة المتطلبات التالية، وتعتبر الشروط التالية شروط رفض للعروض الفنية المقدمة:

- على المتعهد تنفيذ المشروع مفتاح باليد.
- يجب أن تحقق المنظومة جميع المكونات الأساسية للبنية السحابية، الموصفة في الفقرة 4.3، وتعتبر هذه المكونات الشروط الحدود الدنيا المقبولة.
- يجب أن يكون الحل البرمجي للمنظومة من شركة معروفة ومختصة في هذا المجال، ويجب أن تكون جميع المكونات الأساسية للبيئة السحابية متوافقة معاً.
- يجب أن يكون الحل البرمجي للمنظومة متوافق مع نظام التشغيل الملائم المنصب على المخدمات الفيزيائية ويدعم كافة ميزاته.
- يجب أن يكون العرض الفني المقدم من الشركة العارضة مفصّلاً ويشرح بدقّة كافة مكونات الحل مع مخططات تفصيلية له، يتضمن ذلك مخططات تشرح كيفية ارتباط وتفاعل مكونات الحل مع بعضها البعض وتوضعها بالنسبة إلى بعضها البعض (Architectural Overview) و (Logical Overview) و (Components Location) ومخططات التصميم المنطقي للمكونات (Logical Design) لوحدها وفي داخل عناقيد (Clusters) ومخططات التصميم الشبكي المفصلّة للمكونات (Network Design).
- يجب أن تقدم الشركة العارضة Demo حقيقي مستضاف لدى الشركة العارضة أثناء مرحلة دراسة العروض.
- إن شروط الرفض المتعلقة بجزء التجهيزات العتادية موجودة في الجداول التفصيلية المذكورة لاحقاً.

4.4.3. الإطار التشغيلي

يقصد بذلك تحديد المهام والأعمال اللازم القيام بها من قبل العارض لاستمرار عمل المنظومة بعد وضعه في الخدمة، ويمكن تلخيص الأعمال على الشّكل التّالي:

1. يلتزم المتعهد بتشغيل المنظومة وضمان استقرارها وقيامها بجميع وظائفها، وعليه تقديم تقارير دورية للإدارة عن أداء المنظومة.
2. يلتزم المتعهد بتوفير فريق فني مؤهل لمراقبة أداء المنظومة في مقر الاستضافة، وإجراء التدخل السريع خلال فترة التشغيل للأعطال والمشاكل البسيطة التي تحدث أثناء فترة التشغيل، ويحدد في عرضه الفني العدد الكافي لذلك.

3. يلتزم المتعهد بتوفير فريق فني مؤهل للتدخل عن بعد أو في مكان استضافة المنظومة لدى الهيئة لتقديم الدعم الفني لاستمرارية عمل المنظومة، بما يضمن الاستجابة السريعة وتقديم الدعم الفني المتقدم اللازم بكافة الأوقات.
4. يلتزم المتعهد بتوثيق مشاكل التشغيل والحلول المتخذة لمعالجتها، وتقديم تقرير دوري للإدارة بذلك.
5. يلتزم المتعهد بتنفيذ خطة التشغيل وفق المتطلبات الواردة في الفقرة 5.3.

5. توصيف متطلبات المشروع

5.1. المكونات الأساسية للبنية السحابية

تبين الفقرات الآتية كل ما يتعلق بالمكونات الأساسية لمنظومة الحوسبة السحابية، بالإضافة إلى توصيف متطلبات التجهيزات العتادية المطلوبة بحدودها الدنيا، وأخيراً بعض المتطلبات العامة.

5.1.1. مركز البيانات المعرف بشكل برمجي (Software Defined Data Center):

وهو حل برمجي لتقديم موارد المعالجة والتخزين والشبكة والحماية بشكل افتراضي مع منصة لإدارة هذه الموارد المتكاملة.

وحسب تعريفه فإن المكونات الرئيسية لمركز البيانات المعرف بشكل برمجي هي (وهي موصفة تفصيلياً في الفقرات التالية):

1. مكون لتقديم التخزين بشكل افتراضي (Storage Virtualization).
2. مكون لتقديم وإدارة الشبكة وتقديم الحماية بشكل افتراضي (Network and Security Virtualization).
3. مكون لتقديم المعالجة بشكل افتراضي (Compute Virtualization).
4. مكون لتنصيب وإعداد مركز البيانات المعرف بشكل برمجي وتسهيل عمليات الصيانة الدورية للمنظومة من ترقيات وتحديثات.

5.1.1.1. مكون لتقديم التخزين بشكل افتراضي (Storage Virtualization)

هو حل برمجي يقوم بتحويل مخدمات x86 ووحدات التخزين المرفقة معها إلى بنية تحتية هجينة HCI بسيطة، الهدف منها إلغاء التكلفة العالية الموجودة في وحدات التخزين المركزية الشبكية (SAN) بالإضافة إلى إلغاء تعقيدات الإدارة وإلغاء التقييدات في الأداء والتوسع الشاقولي داخل نفس الخزانة أو التوزع على عدة خزانات والتوسع الأفقي من خلال إضافة موارد داخل المخدمات الفيزيائية نفسها.

1. يجب أن يكون الحل البرمجي المقدم متكامل ومتوافق كلياً مع نظام التشغيل المنصب على المخدمات الفيزيائية. ويجب أن يقوم بتجميع كافة الأقراص الموجودة على المخدمات في منظومة عنقودية واحدة (Cluster) بحيث يتم استخدامها كمصفوفة واحدة ذات سرعات عالية لتخزين البيانات الخاصة بالمخدمات الافتراضية التي سوف تنصّب عليها.
2. يجب أن يدعم الحل البرمجي المقدم اتصالات شبكة (Ethernet) ذات السرعات العالية، وألا يعتمد على التوصيلات الضوئية لإنجاز عملياته. مع إمكانية تجميع عدد من المنافذ من كل مخدم فيزيائي موجود في المصفوفة لتشكيل شبكة وصل موثوقة فائقة السرعة.
3. يجب أن يدعم الحل البرمجي المقدم استخدام سياسات وقدرات تخزين معرفة من قبل مدير المنظومة مثل نوع الحماية والتشفير وإلغاء التكرار والضغط ...الخ. وأن تدعم استخدام علامات مميزة لتصنيف وحدات الاستخدام حسب الفئة والقدرات المتاحة فيها.
4. يجب أن يدعم الحل البرمجي المقدم إعدادات All-Flash أو إعدادات Hybrid حسب الحاجة بحيث يكون عدد المخدمات الفيزيائية على الأقل 2، وأن يدعم على الأقل بكل مخدم فيزيائي قرص واحد SSD وقرص واحد HDD بالإضافة إلى إمكانية تقسيم الأقراص في كل مخدم فيزيائي إلى عدة مجموعات (ثلاثة على الأقل) وبكل مجموعة على الأقل 1 cache disk & 5 data disk لتحسين الأداء والفعالية.
5. يجب أن يكون الحل البرمجي متوافقاً مع كافة الميزات المقدمة من نظام التشغيل المنصب على المخدمات الفيزيائية ومتوافقاً مع كافة الميزات المقدمة من قبل مدير المنظومة مثل ميزة توزيع الأحمال التلقائي على المخدمات الفيزيائية (DRS/Storage DRS) وميزة النقل المباشر دون توقف من مخدم فيزيائي لأخر (Live Migration) وميزة توزيع الحمل الكهربائي حسب الحاجة (DPM) وباقي الميزات الأخرى.
6. يجب أن يدعم الحل البرمجي المقدم على الأقل 60 مخدم فيزيائي في كل بنية عنقودية بالإضافة إلى دعم 180 مخدم افتراضي (VM) في كل مخدم فيزيائي بحيث يدعم في كل بنية عنقودية حوالي 6000 مخدم افتراضي (VM) بالإضافة إلى دعم أقراص افتراضية تصل إلى 60 TB من حيث المساحة المستخدمة الفعلية.
7. يجب أن يدعم الحل البرمجي المقدم أنماط الحماية التالية RAID 1/ RAID 5/ RAID 6/ RAID 10 مع إمكانية تحديد نمط الحماية على المخدم الافتراضي (VM) أو على مستوى كل قرص تخزين افتراضي (Virtual Disk/VMDK) في كل مخدم افتراضي.
8. يجب أن يدعم الحل البرمجي المقدم طرق توفير مساحة قابلة للاستخدام مع ضمان الأداء.

<u>الميزات الواجب توفرها في المكون:</u>

1. ميزة الضغط (Compression) وميزة إلغاء التكرار (Deduplication) التي تقوم بتقسيم البيانات إلى قطع صغيرة ثم عمل ترميز لهم (hashing) لها وكتابة الترميز لمرة واحدة.

2. ميزة (Fault Tolerance) وهي الحماية الذاتية والتعافي من الأضرار على مستوى كل مكون موجود في المنظومة (Server\VM\Disk\Port) مع ضمان سلامة البيانات وفق طريقة حماية يحددها مدير المنظومة.
3. ميزة (Fault Domain\ Rack Awareness) وهي ميزة الحماية وسلامة البيانات في حال توقف خزانة كاملة مع كافة مكوناتها من مخدماتها ومبدلات شبكة (Fault Tolerance) لأي سبب كان مع إمكانية تحديد عدد الخزانات الممكن توقفها دون حدوث أضرار على المنظومة من قبل مدير المنظومة وإمكانية تنفيذ هذه الميزة على مستوى المخدم الافتراضي (VM) أو على مستوى كل قرص تخزين افتراضي (Virtual Disk/VMDK).
4. ميزات النسخ والتكرار (Clone and Snapshots) بحيث يمكن صنع عدة نسخ مستقلة من المخدم الافتراضي (Clones) أو عمل عدة نسخ مترابطة من المخدم الافتراضي تحتوي فقط التعديلات بين هذه النسخ (Snapshots). هذه الميزة مفيدة جداً في عمليات النسخ الاحتياطي بالإضافة إلى إرجاع مخدم افتراضي إلى وقت سابق مع ضمان سلامة كافة مكوناته وبياناته. ويجب أن يدعم على الأقل 16000 snapshots في كل clone على مستوى Cluster.
5. ميزة التوفير في المساحة المستخدمة من قبل ملفات التخزين المؤقتة (Swap Efficiency) حيث أن هذه الملفات تستخدم لضمان تلبية متطلبات المخدمات الافتراضية لضمان الأداء خلال فترات الضغط في العمل. هذه الميزة تضمن أن يتم حجز مساحة على قدر الحاجة فقط.
6. ميزة الاستهلاك على قدر الحاجة (Thin provisioning) مع ضمان نفس الأداء المقدم عند استخدام ميزة حجز المساحة المطلوبة كاملة مسبقاً قبل البدء بالاستخدام. ويجب أن يدعم الحل البرمجي إمكانية تفعيل/تعطيل هذه الميزة على مستوى المخدم الافتراضي (VM) أو على مستوى القرص الافتراضي (VMDK/ Virtual Disk).
7. ميزة توزيع عرض الحزمة وعدد العمليات (IOPS) الممكن تنفيذها في كل مكون افتراضي (QoS). وبالتالي ضمان سلامة أداء المنظومة في حال حدوث تصرف غير طبيعي من قبل أي مخدم افتراضي (VM). مع إمكانية عمل عدة مستويات من الأداء (Tiering) وإسنادها إلى المخدمات الافتراضية حسب الحاجة.
8. ميزة التشفير من خلال دمجه مع حل يقوم بإدارة مفاتيح التشفير وذلك من أجل حماية البيانات من السرقة.
9. يجب أن يدعم الحل البرمجي المقدم سرعات عالية في الأداء والموثوقية بحيث يلائم كافة المتطلبات لكافة البيئات والتطبيقات المستخدمة في الشركات والمنظمات الكبرى.
10. إمكانية الإدارة من مكان مركزي واحد من خلال دمجه مع المخدم الافتراضي المسؤول عن إدارة كامل المنظومة بالإضافة إلى القدرة على مراقبة الأداء الفيزيائي والافتراضي لكافة المكونات (Hardware\Disks\Network\Cache\Ports) واكتشاف مناطق الضعف والتي تحتاج إلى ترقية أو زيادة في العدد.
11. يجب أن يدعم الحل البرمجي المقدم إمكانية دمجه مع برامج المراقبة الأخرى وبرامج مراقبة التحذيرات (alert monitoring) وإرسال إشعارات وتحذيرات عند حدوث المشاكل إلى المسؤولين عن المنظومة.

12. إمكانية إنجاز أعمال صيانة على المخدمات الفيزيائية دون الحاجة إلى عمل أي تغييرات في الإعدادات مع ضمان سلامة البيانات وفعالية الأداء على كامل المنظومة.
13. خدمات مشاركة الملفات (NAS) والذي يقدم تشاركية للملفات بين المخدمات الافتراضية (VM) باستخدام بروتوكولات SMB v2.1/SMB v3/ NFS 3/ NFS v4.1 بالإضافة إلى إمكانية دمجه مع AD/Kerberos.
14. إمكانية الترقية وتنزيل التحديثات (Software\Firmware\Driver) لكافة المكونات بشكل مباشر دون الحاجة إلى التوقف.
15. الدعم لمشغل التطبيقات الحديثة الذي يمكن الوصول إلى الحاويات البرمجية المعدة مسبقاً (Containers) حسب الحاجة والتي تسرع عملية تقديم الخدمات إلى المشتركين.

5.1.1.2. مكون إدارة الشبكة والحماية بشكل افتراضي (Network and Security Virtualization)

هو مكون أساسي من مكونات بنية المعالجة السحابية يقدم العديد من الخدمات الأساسية لعمل بنى مراكز البيانات الافتراضية (SDDC) بشكل برمجي ومؤتمت حسب الحاجة ويحقق بالتالي توفير كبير في تكاليف المعدات والتجهيزات المطلوبة لاستمرارية العمل بالإضافة إلى المرونة العالية في الاستجابة لمتطلبات العمل الشبكية ويقدم الحماية بشكل مؤتمت وبطريقة برمجية. وتتم إدارة كافة مكونات الشبكة والحماية من مكان مركزي.

<u>الميزات الواجب توفرها في المكون:</u>

1. تحقيق الإتاحية والاستمرارية (HA) من خلال تركيب مكوناته بطريقة عنقودية (Cluster) وبالتالي تجنب توقف المنظومة عند حدوث خلل ما وتجنب وجود نقطة فشل وحيدة في المنظومة.
2. يجب أن تكون مكوناته جاهزة ومعدة للتنصيب خلال دقائق وأن تكون من شركة عالمية معروفة وموثوقة وذات كفاءة عالية مع إمكانية تحديث مكوناته وتنزيل التحديثات الأمنية بطريقة مباشرة دون الحاجة إلى إيقاف عمل المنظومة.
3. إمكانية عمل التعديلات على الشبكة الافتراضية في زمن قصير (دقائق) دون الحاجة إلى التغير في الشبكة الفيزيائية وبشكل مرن وبرمجي وأن يكون مستقل عن الشبكة الفيزيائية.
4. إمكانية عمل تعديلات برمجية على المنظومة وأتمتة كافة العمليات التشغيلية عليه عند الحاجة من خلال توفيره واجهة برمجية Restful API.
5. أن تقوم مكوناته بعمل بنية شبكية (Fabric/Overlay) مكونة من المخدمات الفيزيائية نفسها دون الحاجة إلى أي مكونات شبكية فيزيائية بحيث يكون كل عنصر من هذه البنية عبارة عن مبدل شبكي افتراضي وموجه شبكة افتراضي وجدار حماية افتراضي ومكتشف ثغرات واختراقات أمنية افتراضي وموزع أحمال افتراضي ... الخ.

6. أن تكون البنية (Fabric/Overlay) تدعم 1000 مخدم فيزيائي يمكن تقسيمها إلى حوالي 100 بنية عنقودية (Cluster) ممكن أن تعطي 10000 مبدلة افتراضية (logical switches) و 10000 مقطع شبكي منطقي معزول ومفصول (Segment) وإمكانية ربط مع شبكات فيزيائية مفصولة (Bridging) تصل إلى 4000 و160 موجه افتراضي (virtual router) يمكن ربطه مع الشبكة الفيزيائية بالإضافة 4000 موجه منطقي مستخدم داخل البنية الافتراضية و أن يدعم حوالي 25000 سياسة تحويل شبكي (NAT Rules) و 4000 موزع عناوين شبكة مؤتمت (DHCP) و دعم 100000 سياسة حماية شبكية (Stateful Firewall Rules) يمكن تقسيمهم إلى 10000 قسم أمني بكل قسم يدعم 1000 سياسة أمنية.
7. إمكانية إنشاء شبكات طبقة ثانية (Layer 2) افتراضية بطريقة برمجية وسريعة في أي مكان ضمن البنية (Fabric) بغض النظر عن مكان المخدم الفيزيائي وطريقة وصله.
8. إنجاز عمليات التوجيه (routing) بين مقاطع الشبكة المختلفة (IP subnets) دون الحاجة إلى الولوج إلى الموجه الفيزيائي (Router).
9. إنجاز عمليات التوجيه في طبقة نظام التشغيل المنصب على المخدم الفيزيائي باستخدام جزء بسيط من موارده وبالتالي تسريع عمليات نقل البيانات بين المخدمات الافتراضية (VM) الموجودة ضمن المقطع الشبكي نفسه (Segment) أو في مقاطع شبكية مختلفة ضمن البنية (Fabric).
10. إنجاز عمليات الحماية الموزعة من مكان مركزي (Distributed Firewall) وعلى مستوى كرت الشبكة الخاص بكل مخدم افتراضي موجود في البنية (Fabric) بأقل تكاليف الموارد ويفضل أن تكون جزء من نظام التشغيل المنصب على المخدمات الفيزيائية لتوفير أداء عالي جداً وبسرعات قياسية.
11. تقديم وإنجاز عمليات توزيع الأحمال (load balancing) على المخدمات الافتراضية دون الحاجة إلى معدات فيزيائية ودون الحاجة إلى التعديل في الشبكة الفيزيائية. يجب أن تدعم عملية توزيع الأحمال العمل في عدة طبقات شبكية (Layer 4 – Layer 7) مع إمكانية التزويد بإخماد التشفير (SSL termination).
12. تقديم خدمات الشبكات الافتراضية الخاصة (VPN) في طبقات الشبكة الثانية والثالثة (L2 & L3) بين عدة مواقع شبكية ضمن البنية (Fabric) أو خارجها ضمن أنفاق حماية مشفرة SSL.
13. إمكانية ربط عدة مواقع معاً (Site-to-Site) عن طريق أنفاق مشفرة ومؤمنة (Tunnel) باستخدام شبكات افتراضية خاصة مشفرة ومحمية (IPsec VPN).
14. توسيع قدرات وحدود الشبكة الافتراضية إلى خارج البنية (Fabric) وإمكانية دمجها مع الشبكة الفيزيائية عند الحاجة.
15. تقديم خدمات الوصول عن بعد للمستخدمين بطريقة برمجية ومشفرة عن طريق عمل شبكات خاصة ومؤمنة بين الطرفين باستخدام.

16. إمكانية دمجه مع حلول أمنية أخرى مثل مضاد الفيروسات بحيث تصبح عمليات الحماية من البرمجية الخبيثة مؤتمتة فيقوم هذا المكون بعزل شبكي لأي مخدم افتراضي (VM) يشتبه بإصابته وعزله في مكان شبكي منفصل خاص به.
17. إمكانية عمل نسخ احتياطية واسترجاع لإعدادات المكون الافتراضي من أجل التعافي من الكوارث عند الحاجة أو في حال حدوث خطأ بشري في الإعدادات.
18. دعم عملية التنصيب والإعداد التلقائي المؤتمت لمكوناته على المخدم الفيزيائي في حال إضافة أو إزالة أي مخدم فيزيائي من المنظومة العنقودية (Cluster).
19. دعم عمليات الترقية والتحديث لكافة مكوناته على المخدمات الفيزيائية أو لمكوناته الافتراضية من مكان مركزي ودون حدوث أي انقطاع في منظومة العمل.
20. أن يدعم الاتحادية (Federation) بحيث يمكنك ربط عدة مواقع فيزيائية منفصلة وإدارتها على أنها موقع وحيد وإمكانية نقل المخدم الافتراضية بين هذه المواقع بشكل مؤتمت دون الحاجة إلى عمل أي تعديلات في الشبكة الفيزيائية بالإضافة إلى إمكانية تجزئة هذه الاتحادية إلى قطاعات منطقية (Zones) لتؤدي كافة المتطلبات الشبكية المطلوبة حسب الحاجة.
21. أن يدعم عمليات التخزين المؤقت لطلبات تحويل الأسماء إلى عناوين (DNS Caching) وإمكانية تحديد مجالات الأسماء التي ترغب بعمل تخزين مؤقت لها.
22. أن يدعم إنشاء مخدمات توزيع العناوين التلقائية (DHCP Servers) وتخصيص عملية العنونة حسب مقطع الشبكة القادم منها الطلب بالإضافة إلى إمكانية طلب عناوين من المخدمات خارج الشبكة الافتراضية أو داخلها (DCHP relay).
23. أن يدعم عمليات تحويل وتغير عناوين الشبكة (NAT) على مستوى المنفذ أو العنوان وبكلا النوعين عملية التحويل/تغير عنوان/منفذ المصدر (SNAT) والنوعين عملية التحويل/تغير عنوان/منفذ المستهدف (DNAT).
24. دعم إمكانية اكتشاف ومنع البرمجيات الطفيلية (IDS/IPS) بشكل برمجي وموزع على كامل المنظومة وليس ضمن الحدود الخارجية لها فقط وتعريف السياسات الخاصة بها على أدنى مستوى في الشبكة الافتراضية وهو كرت شبكة المخدم الافتراضي مع إمكانية إسناد هذه السياسات بشكل ديناميكي إلى المخدمات الافتراضية عن طريق استخدام الأوسمة والعلامات الدالة (tags) بحيث تبقى السياسات نفسها مطبقة على المخدم الافتراضي أينما نقل ضمن الشبكة وضمن المنظومة.
25. أن يدعم عملية تحليل روابط مواقع الشبكة العنكبوتية وتحليلها وتصنيفها وعمل تقارير بحيث تمكن المسؤول من معرفة أنماط مواقع الويب التي يتم الوصول اليها من داخل الشبكة.
26. دعم بروتوكولات إدارة الشبكة (SNMP) وإمكانية ارسال التحذيرات والاشعارات إلى برامج مراقبة مركزية معدة لهذا الغرض.

27. إمكانية إعداده وبرمجة مكوناته وميزاته عن طريق لغات البرمجة العالمية المختصة في برمجة مراكز البيانات الافتراضية والفيزيائية مثل Ansible & Terraform.
28. أن يكون لديه مكون رديف يسمح برؤية كافة حركات نقل البيانات ضمن الشبكة الافتراضية والفيزيائية مع تقديم المساعدة في عمليات تخطيط العمليات والتصميم والتركيب والتعديل في السياسات الأمنية وتقديم النصائح والإرشادات بشكل دوري وإمكانية اكتشاف الأخطاء التقنية والفنية الموجودة في الإعدادات بالإضافة من القدرة على التأكد من الإطاعة والتقيد بالسياسات الأمنية الموضوعة من قبل الإدارة مع القدرة على مراقبة التعديلات الحاصلة على مكونات الشبكة ومعرفة من قبل من تم التعديل وبأي تاريخ حصل التعديل بالإضافة إلى إمكانية البحث باستخدام معايير عن أي مكون ضمن الشبكة والبنية ورؤية كافة معلوماته التفصيلية من حيث الشبكة والحماية وطريقة الوصل ومقدار التدفق.
29. أن يدعم المكون الرديف عمليات تجميع المعلومات الخاصة بالأداء للشبكة الافتراضية والفيزيائية وإمكانية عرض هذه المعلومات بعدة طرق بالإضافة إلى دعم عملية مراقبة محتوى البيانات المتدفقة عبر الشبكة وإمكانية توجيه نسخة منها إلى جهاز آخر لعمل تدقيق ومراقبة مع إمكانية إعطاء تسميات منطقية لعمليات النقل بحيث تصبح عملية التحليل أسهل وهذه التسميات قد تكون حسب طريقة عمل المخدم الافتراضي أو حسب طبيعة حركة النقل فيه. بالإضافة إلى خرائط ديناميكية للشبكة تظهر حركة نقل البيانات وكيفية حصول التدفق عبر الشبكة والتواصل بين المكونات الفيزيائية والمكونات الافتراضية.
30. أن يدعم المكون الرديف تجميع المخدمات الافتراضية في مجموعات حسب طبيعة عملهم بطريقة ديناميكية تكون معرفة بسياسات ومعايير تحدد من قبل مدير المنظومة بالإضافة إلى إمكانية تعريف وتخصيص الشعارات وتنبيهات عند حدوث حركة نقل ما أو عند حصول حدث معين ضمن المنظومة.

5.1.1.3. مكون تقديم المعالجة بشكل افتراضي (Compute Virtualization)

هو نظام تشغيل خاص بالبنى الافتراضية ينصب مباشرة على المخدمات الفيزيائية دون الحاجة لوجود أي نظام تشغيل وسيط. يقوم بإدارة العتاد الصلب والموارد الفيزيائية ويوفر القدرة على إنشاء أكثر من مخدم افتراضي واحد على المخدم الفيزيائي نفسه من خلال خلق تشاركية في الموارد لتوفير التكلفة وفصل بين المخدمات الافتراضية (VMs) لتأمين الحماية. من ميزات المخدمات الافتراضية (VMs) سهولة التركيب والصيانة وانخفاض الكلفة التشغيلية بالإضافة إلى المرونة في عمليات النسخ الاحتياطي والصيانة والنقل من مخدم فيزيائي إلى مخدم آخر ومن مكان جغرافي إلى مكان آخر دون توقف مع إمكانية عمل نسخ لحظية زمنية تمكن من العودة إلى نقطة زمنية محددة مسبقاً.

<u>الميزات الواجب توفرها في المكون:</u>

1. يجب أن يكون من نوع النمط الأول الذي لا يعتمد على نظام تشغيل آخر حاضن له.

2. يجب أن يكون له تحديثات دورية قابلة للتنصيب دون الحاجة إلى إيقاف العمل وأن تكون عملية الترقية والتحديث مركزية ومرنة وسهلة التنفيذ.
3. يجب أن يكون لديه واجهة إدارة يمكن الوصل لها عن طريق مستعرض الانترنت دون الحاجة لتنزيل أي أدوات إضافية بحيث تمكن هذه الواجهة من إدارة المخدمات الافتراضية ومواردها الشبكية والتخزينية.
4. أن يكون لديه مكون رديف يمكنك من عمل بنية عنقودية من عدة مخدمات فيزيائية بحيث تفعل ميزات الحماية والتشاركية والحفاظ على المعلومات وعلى إبقاء المنظومة تعمل عند حدوث فشل وحيد.
5. يجب أن يدعم بكل إمكانية إنشاء 1024 مخدم افتراضي (VMs) بكل مخدم فيزيائي.
6. يجب أن يدعم الميزات الفنية التالية بكل مخدم افتراضي (VM):
   - عدد وحدات معالجة مركزية افتراضية (vCPUs) يصل حتى 760.
   - حجم ذاكرة وصول عشوائية مؤقتة (vRAM) تصل حتى 20TB.
   - حجم ملف تبادلي مساعد للذاكرة الوصول العشوائية (Swap) يصل حتى 20TB.
   - عدد أقراص تخزين افتراضية (Virtual Disks) تصل حتى 60 قرص.
   - حجم قرص التخزين الافتراضي الواحد يصل حتى 60 TB.
   - عدد الأجهزة الطرفية التي يمكن وصلها يصل حتى 20.
   - عدد المنافذ التسلسلية يصل حتى 20.
   - عدد منافذ شبكية يصل حتى 10.
   - ذاكرة وصول عشوائية ثابتة تصل حتى 12TB.
7. يجب أن يدعم الميزات الفنية التالية بكل مخدم فيزيائي:
   - عدد وحدات معالجة مركزية افتراضية (CPUs) يصل حتى 760.
   - حجم ذاكرة وصول عشوائية مؤقتة (RAM) تصل حتى 20TB.
   - ذاكرة وصول عشوائية ثابتة (persistent Memory) تصل حتى 12TB.
   - عدد منافذ الشبكة المدعومة حسب السرعة كالتالي:
     - سرعة 1 Gbps يصل حتى 32 منفذ شبكة.
     - سرعة 10 Gbps يصل حتى 16 منفذ شبكة.
     - سرعة 25 Gbps يصل حتى 16 منفذ شبكة.
     - سرعة 40/50 Gbps يصل حتى 8 منفذ شبكة.
   - عدد منافذ شبكة افتراضية كلي يصل حتى 4096.
8. دعم عملية توزيع الصلاحيات على المستخدمين حسب مهمته (RBAC) مع إمكانية ربطه مع مدقق حسابات/هوية خارجي مثل Microsoft Active Directory.

9. دعم عملية تشغيل الحاويات البرمجية الجاهزة (Containers) بشكل موثوق وآمن مع توفير كل ما تحتاجه من موارد شبكة وتخزين من خلال المكونات الرديفة له.

5.1.1.4. مكون إدارة مركز البيانات المعرف بشكل برمجي

هو مكون برمجي معد مسبقاً ومنصب على نظام تشغيل خاص به من الشركة المصنعة وجاهز للاستخدام مباشرة، مهمته إدارة كافة المكونات والموارد الخاصة بالمخدمات الافتراضية الموجودة على المخدمات الفيزيائية.

من خلال دمجه مع نظام التشغيل المذكور سابقاً الذي ينصب على المخدمات الفيزيائية يمكن تجميع المخدمات الفيزيائية في بنى عنقودية (Clusters) ثم تقسيم مواردها إلى عدة مجموعات موارد (Resource Pools) بحيث يمكن تقسيم هذه المجموعات إلى عدد من المستويات حسب الحاجة.

يدعم إمكانية إنشاء حسابات المستخدمين ومجموعات مستخدمين (Users & Groups) وإسناد وتوزيع الصلاحيات إليهم حسب وظيفة كل منهم (RBAC) مع إمكانية ربطه مع مدقق حسابات/هوية خارجي مثل Microsoft Active Directory.

<u>الميزات الواجب توفرها في المكون:</u>

1. يجب أن يكون له تحديثات دورية قابلة للتنصيب دون الحاجة إلى إيقاف العمل وأن تكون عملية الترقية والتحديث مركزية ومرنة وسهلة التنفيذ.
2. يجب أن يكون لديه واجهة إدارة يمكن الوصل لها عن طريق مستعرض الإنترنت دون الحاجة لتنزيل أي أدوات إضافية وهذه الواجهة تمكن من إدارة المخدمات الافتراضية وموارد الشبكية والتخزينية.
3. يدعم عملية تجميع المخدمات الفزيائية في بنى عنقودية (Clusters) لضمان الإتاحية والتكاملية والحماية من وجود نقطة فشل وحيدة في المنظومة.
4. دعم عملية تجميع الموارد الفيزيائية في مجموعات (Resource pool) وعمل تشاركية بينهم وإمكانية إنشاء مخدمات افتراضية تستخدم هذه الموارد حسب المعايير التي يحددها مدير المنظومة.
5. يجب أن يدعم تشغيل وإدارة مخدمات افتراضية (VMs) تصل حتى 40000.
6. يجب أن يدعم عدد اتصالات إلى واجهته الإدارية يصل حتى 100 اتصال بنفس الوقت.
7. أن يكون لديه ميزة حماية ذاتية بحيث تنشأ أكثر من نسخة منه متزامنة معا تمنع وجود نقطة فشل وحيدة في المنظومة. في حال توقف النسخة الأساسية تحل محلها النسخة الثانوية ويتم إنشاء نسخة جديدة منها تلعب دور النسخة الثانوية لضمان الإتاحية بشكل دائم.
8. يجب أن يكون لديه واجهة إدارية خاصة يتم الوصول اليها عن طريق مستعرض الانترنت تمكنك من إنجاز عمليات الاعداد والصيانة وعمل الترقيات والتحديثات لكافة مكوناته.

9. يجب أن يدعم إمكانية عمل نسخ احتياطية منه بشكل دوري معرف من قبل مدير المنظومة وتخزينهم خارج المنظومة مع إمكانية استخدام هذه الملفات لإعادة تنصيب واحدة جديدة بنفس الاعدادات التي كانت موجودة.
10. يجب أن يكون لديه نظام تسجيل دخول وحيد مشفر محمي ومؤمن يمكن المستخدمين من تسجيل الدخول لمرة واحدة (SSO) وإنجاز كافة المهام الإدارية المسموح لهم بها دون الحاجة لإعادة تسجيل الدخول بكل مرة يتم فيها الانتقال من مكون إلى مكون أخر ضمن المنظومة.
11. يجب أن يكون لديه محرك بحث يمكنك من الوصول إلى المكون الذي تريده ضمن المنظومة عن طريق اسمه أو عنوانه أو العلامة الدالة الموضوعة عليه (Tags).
12. يجب أن يتمكن من إرسال التحذيرات والبلاغات عند حدوث أمر ما مع إمكانية تخصيص هذه الإشعارات بالإضافة إلى إمكانية إرسالها عبر البريد الالكتروني أو إرسالها إلى نظام رديف يقوم بقدح إجرائية معرفة مسبقاً وفق الحدث الذي تم.
13. يجب أن يدعم ميزة إنشاء معايير وسياسات لإعدادات المخدمات الفيزيائية (Host profiles) بحيث يمكن من إعداد أي مخدم جديد مباشرة بشكل مؤتمت وفق السياسة المسندة له مع إمكانية التحقق من خضوع المخدمات الفيزيائية للسياسات الفنية والأمنية الموكلة له مع إمكانية إعادة تطبيق وفرض السياسة من جديد في حال عدم الاطاعة لها وبالتالي ضمان تناسقية ونزاهة الإعدادات على كافة المخدمات الفيزيائية.
14. إدارة موارد المخدمات الافتراضية (VM) وتحديد مقدار الاستهلاك الأعلى المسموح به لكل مخدم افتراضي مع تحديد الأولويات عند حدوث اختناق في استهلاك الموارد مع إمكانية تعديل مقدار الموارد المستهلكة من قبل المخدم الافتراضية دون الحاجة إلى إيقاف عمل المخدم الافتراضي.
15. يجب أن يدعم ميزة مراقبة المخدمات الافتراضية (VM) وفي حال توقفها لسبب داخلي أن يقوم بإعادة تشغيلها تلقائياً وفي حال غيابها عن المنظومة بسبب توقف المخدم المضيف الحاضن لها أن يقوم بإعادة تشغيل المخدم الافتراضي على مخدم فيزيائي أخر مع ضمان عدم وجود نسختين من المخدم الافتراضي لضمان سلامة البيانات.
16. يجب أن يدعم ميزة توزيع أحمال الاستهلاك في موارد المخدمات الافتراضية (VM) على المخدمات الفيزيائية بشكل متساوي ومتناسق وحسب مجموعة معايير مثل نسبة استهلاك وحدات المعالجة المركزية أو/وكمية استهلاك الذواكر الوصول العشوائي أو/وعدد المخدمات الافتراضية التي تعمل حالياً.
17. يجب أن يدعم ميزة توزيع أحمال استهلاك التخزين الخاصة بالمخدمات الافتراضية (VM) على وحدات التخزين المركزية بشكل متساوي ومتناسق.
18. يجب أن يدعم ميزة إطفاء وتشغيل المخدمات الفيزيائية تلقائياً حسب مقدار استهلاك الموارد الفيزيائية فيها بحسب معايير يتم وضعها من مدير المنظومة.
19. يجب أن يدعم ميزة تخصيص وتقسيم عرض حزمة الشبكة الفيزيائية إلى باقات وإسناد هذه الباقات إلى المخدمات الافتراضية (VMs) حسب أهميتها مع ضمان حصول المخدمات الافتراضية على الحزم والباقات المخصصة لها أينما نقلت ضمن البنية التحتية.

20. يجب أن يدعم تخصيص وتقسيم عرض حزمة شبكة نقل البيانات إلى وحدات التخزين إلى باقات وإسناد هذه الباقات إلى المخدمات الافتراضية (VMs) حسب أهميتها مع ضمان نفس حصول المخدمات الافتراضية على الحزم والباقات المخصصة لها أينما نقلت ضمن البنية التحتية.
21. يجب أن يدعم ميزة نقل المخدمات الافتراضية (VMs) من مخدم فيزيائي إلى أخر بشكل لحظي ودون توقف عمل المخدم الافتراض وإمكانية دمجها مع الميزات المذكورة سابقا ليتم توزيع الأحمال على المخدمات الفيزيائية بشكل أتوماتيكي ودون حدوث أي توقف في عمل المخدمات الافتراضية.
22. يجب أن يدعم خدمات الجيل الجديد من الحاويات التشغيلية (Containers) بحيث يمكنك من تشغيل الحاويات البرمجية على المخدمات الفيزيائية بشكل مباشر دون الحاجة إلى وسيط وتأمين كافة المستلزمات التقنية التي تمكن هذه الحاويات من العمل بدون وجود أي نقطة فشل وحيدة في المنظومة.
23. يجب أن يدعم إمكانية تشغيل أكثر من نسخة منفصلة من المخدمات الافتراضية على المخدمات الفيزيائية بحيث يضمن دائماً وجود نسخة تعمل في حال حدوث أي مشكلة فنية.
24. يجب أن يدعم ميزة الربط مع مكون رديف يمكن من عمل مزامنة للمخدمات الافتراضية ضمن الموقع أو بين عدة مواقع.
25. يجب أن يدعم برمجياً وحدات التخزين الخارجية المؤسساتية بحيث يتم نقل أعباء (offload) تنفيذ عمليات النسخ والتخزين والعمليات التخزينية الأخرى من المخدمات الفيزيائية إلى وحدات التخزين المركزية.
26. يجب أن يدعم عمليات التشفير والحماية للمخدمات الافتراضية وفق أحدث المعايير العالمية.
27. يجب أن يدعم عملية إعداد وتركيب المخدمات الفيزيائية الجديدة بشكل تلقائي عن طريق الشبكة من خلال تحضير البنية التحتية الملائمة لذلك.
28. يجب أن يدعم إمكانية إدارة المنظومة بشكل برمجي من خلال توفير نوافذ برمجية تمكن لغات برمجة مراكز البيانات المعروفة عالميا مثل Terraform/Ansible/Chefمن انجاز العمليات بشكل مؤتمت.
29. يجب أن يدعم ميزة إنشاء مكتبات لتخزين الملفات والأقراص الليزرية (ISO files) وقوالب المخدمات الافتراضية (vApp/OVA Files) مع إمكانية مشاركتها.

5.1.2. مكونات أتمتة وإدارة البنية السحابية

هي مجموعة من البرمجيات المتناغمة التي تؤمن إدارة البنية السحابية بطريقة مؤتمتة وبسيطة مع إمكانية عمل تخصيصات لكل مؤسسة من المؤسسات المُستضافة ضمن البنية السحابية. بالإضافة إلى توفير المرونة في التوسيع عند الحاجة دون الحاجة الى أي توقف في البنية.

تمكّن هذه المكونات من إعداد عدة مراكز بيانية فيزيائية موزعة على عدة أماكن فيزيائية منفصلة جغرافياً من مكان واحد وتقسيم هذه الموارد إلى عدة هيئات منطقية بحيث يمكن أن يكون لكل هيئة مركز بيانات افتراضية واحد أو أكثر حسب الرغبة، وقد يكون هذا المركز موزع على عدد من الأماكن الفيزيائية حسب رغبة المؤسسة.

تمكّن هذه المكونات من رؤية حالة كافة المكونات الافتراضية في البنية وتمكّن كل منظمة من رؤية المكونات الافتراضية الخاصة بها وطريقة أداءها، مع إمكانية التخصيص والأتمتة حسب الرغبة بالإضافة الى إظهار تكلفة كل مكون افتراضي موجود في مراكز بيانات الافتراضية للهيئة بحيث يمكن المسؤولون في الهيئة من معرفة التكاليف التشغيلية والإصلاحية لكل مكون وتطبيق موجود لديهم ضمن فترات زمنية يمكن تحديدها حسب الحاجة وكل ذلك من خلال واجهات بسيطة وسهلة الاستخدام.

يستطيع المسؤولون من خلال هذه المكونات في كل هيئة إنجاز عمليات الصيانة والنسخ الاحتياطي لكافة المكونات الافتراضية الموجودة لديهم في مراكز البيانات الافتراضية بطرق مؤتمتة وباستخدام واجهات بسيطة وسهلة الاستخدام. بالإضافة الى التنبؤ بالأخطار والمشاكل التي سوف تظهر مستقبلاً واظهار إحصائيات حول مقدار الموارد المطلوبة لاحقاً على فترات زمنية معينة يتم تحديدها من قبل المسؤولين.

يمكن تقسيم هذه المكونات من حيث المهمة الى الأقسام التالية:

1. مكون الإدارة المركزي.
2. مكون مراقبة الأحداث.
3. مكون مراقبة الأداء والتنبؤ والاحصائيات.
4. مكون الأتمتة.
5. مكون نظام الفوترة.
6. مكون الحماية والإتاحة.

5.1.2.1. مكون الإدارة المركزي

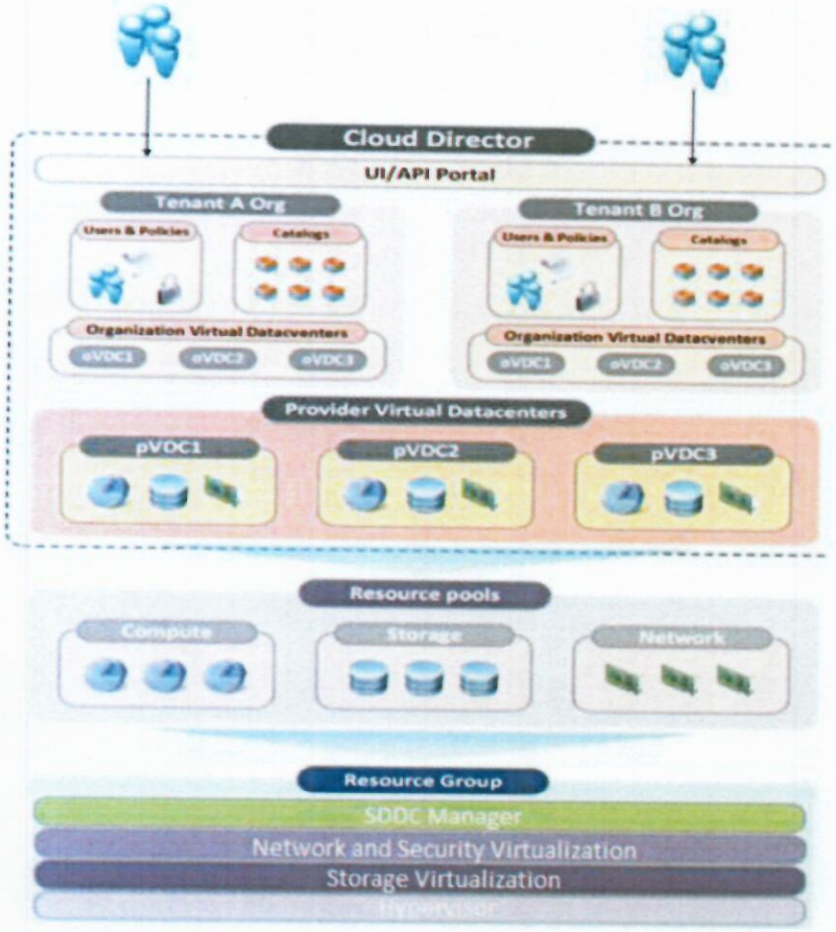
هو المكون والمحرك الأساسي لعمليات إدارة وأتمتة وتنظيم البنية السحابية، يمكنه لعب دور مزود الخدمة للبنى السحابية بكافة أشكالها: الخاصة والعامة والهجينة. فهو الذي يمكن مزود الخدمة السحابية من تقديم الخدمات للمنظمات والمؤسسات من خلال تقديم مراكز بيانات افتراضية معزولة عن بعضها البعض ومحمية ومؤمنة مع وجود فصل في الموارد من حيث موارد المعالجة والتخزين والشبكة وجدران الحماية والسياسات الأمنية والتخزينية والتوجيهية والسياسات التقنية الأخرى.

<u>الميزات الواجب توفرها في المكون:</u>

1. يمكن للمنظمات والمؤسسات إنشاء قوالب مخدمات افتراضية (VM Template) أو مجموعة واحدة من المخدمات الافتراضية التي تقدم معاً برمجيات عالية المستوى (vApps Template) وتجميعها معاً في دليل مفهرس للخدمات

(Catalog) بحيث يمكن للمستخدمين الموجودين في هذه المؤسسة تركيب هذه البرمجيات واستخدامها في دقائق مع إمكانية رؤية تكلفة هذه الخدمات وفق فترات زمنية متنوعة وإمكانية إزالة الخدمة في دقائق أيضاً.

2. أتمتة عمليات إعداد الشبكة وسياسات الحماية للمؤسسات والهيئات عند تركيب أي برمجيات وبرامج جديدة من خلال الاعتماد على مكون إعداد الشبكة البرمجي المذكور سابقاً بالإضافة إلى تقديم خدمات شبكية أخرى مثل: NAT/Routing/Firewall Rules/DHCP/DNS..
3. تمكين المستخدمين الموجودين في المؤسسات من الوصول إلى الخدمات والبرمجيات المتاحة لهم من قبل منظمتهم عن طريق مستعرض الويب من أي جهاز لديه نظام تشغيل ذكي ودون الحاجة الى أي برمجيات رديفة ومن أي مكان مسموح به وفق سياسات الحماية التي تحددها المنظمة/المؤسسة.
4. تمكين المؤسسات/المنظمات من تركيب وتقديم الخدمات البرمجيات من عدة أماكن منفصلة جغرافياً وتمكين المستخدمين من الاستفادة من هذه الخدمات في أي مكان.
5. تمكين المسؤولين في المنظمات/المؤسسات من تقسيم صلاحيات المستخدمين في المنظمة الخاصة بهم واعطاءهم صلاحيات حسب دورهم وحسب البرمجيات التي يريدون استخدامها.
6. تمكين المسؤولين في المنظمات/المؤسسات من مراقبة حالة البرمجيات ومراكز البيانات الخاصة بهم بكافة مكوناتها الشبكية والتخزينية والأمنية والبرمجية وإمكانية عمل النسخ الاحتياطية والنسخ الرديفة إلى مواقع أخرى بشكل برمجي ومؤتمت بالإضافة الى توليد اشعارات وفق معايير معينة تحدد من قبل المسؤولين وتحديد طريقة توصيل الإشعارات.
7. المثال التالي يوضح شكل البنية المنطقية للبنية السحابية المطلوبة:



8. إمكانية تقسيم مراكز البيانات الفيزيائية الى عدة هيئات/مؤسسات منطقية بحيث يمكن أن يكون لكل هيئة/مؤسسة غرفة بيانات خاصة بها واحدة أو أكثر حسب متطلبات الهيئة. وأن تكون هذه الغرف معزولة ومفصولة عن بعض البعض مع إمكانية إعطاء أعضاء الهيئة صلاحيات على مستوى المنظمة/الهيئة الخاصة بهم فقط.
9. إعطاء المسؤولين عن المؤسسة/الهيئة إمكانية إنشاء مراكز البيانات الافتراضية الخاصة بهم وإعدادهم بالطريقة التي يرغبون بها وتحديد نوع التطبيقات والبرمجيات والخدمات المتاحة التي يرغبون بها من دليل البنية السحابية العام (Cloud Catalog) مع إمكانية إنشاء خدمات خاصة بهم مع إمكانية إسناد الصلاحيات إلى المستخدمين الخاصة بهم حسب الحاجة.
10. تمكين المسؤولين في المنظمات/المؤسسات من مراقبة حالة البرمجيات ومراكز البيانات الخاصة بهم بكافة مكوناتها الشبكية والتخزينية والأمنية والبرمجية وإمكانية عمل النسخ الاحتياطية والنسخ الرديفة إلى مواقع أخرى بشكل برمجي ومؤتمت بالإضافة إلى توليد إشعارات وفق معايير معينة تحدد من قبل المسؤولين وتحديد طريقة توصيل الإشعارات: بريد الكتروني / رسائل نصية / تشغيل اجرائيات معينة.

11. تمكين المسؤولين في المنظمات/المؤسسات من رؤية التكاليف التشغيلية الحالية في مراكز البيانات الافتراضية الخاصة بهم وعلى مستوى كل برنامج/خدمة لديهم مع عرض تكاليف التشغيل والصيانة عند تركيب/إزالة خدمة وانعكاس هذا التغير والتعديل على كامل المنظومة الخاصة بهم.
12. تمكين المسؤولين عن إدارة البنية السحابية من رؤية احصائيات استخدام كل منظمة وتأثير ذلك على المنظومة وطباعة تقارير مالية وفنية عن حالة المنظومة الفزيائية والبنى الافتراضية.
13. إمكانية أتمتة العمليات وتقديمها كخدمة عن طريق خدمة workflow الموجودة ضمن المنظومة حيث يستطيع المسؤولين عن المنظمة القيام بوضع السكريبت الذي يريدون دمجه ضمن نظام الأتمتة workflow.
14. يستطيع أعضاء الهيئة القيام برؤية عمليات Restore & Backup التي تحصل ضمن المنظمة وغرف البيانات الافتراضية الموجودة لديهم بالإضافة إلى إمكانية التحكم بهم حسب الحاجة بطريقة سهلة وعن طريق سياسات يقوم المسؤول عن المنظمة بوضعها ودون الحاجة لأن يكون المسؤولين خبراء في العمليات.
15. إمكانية تعريف مجموعة من أنظمة التشغيل مع برامجها وعمل تخصيص لهم وقت الحاجة وتخزينها ضمن حزمة واحدة بحيث يمكنها العمل كمنظومة واحدة معاً متضمنة التطبيقات/مساحة التخزين/ الشبكة والحماية بسهولة وسرعة.
16. يجب أن تدعم المنظومة عدة أنماط من الاستهلاك لموارد غرفة البيانات الفيزيائية وإمكانية التقسيم حسب هذه الآليات:
    - Pay as you go: الدفع حسب الاستهلاك حيث أن المنظمة لا يكون لديها شيء محجوز وإنما يتم الحجز عند الطلب وبالتالي توفير عالي في الموارد مع تحقيق عائدات مالية أكبر وأفضل وبحيث تضمن تحقيق الخدمة المطلوبة بما يتناسب مع الاتفاقية الموقعة مع الزبون (SLA) بالحد الأدنى.
    - Allocation pool of resources: تخصيص حزم استهلاك معينة كنظام الباقات بنسب مئوية بحيث تضمن دائماً وجود الموارد المطلوبة الدنيا وتحقق الجودة وفق ما هو مذكور في الاتفاقية الموقعة مع الزبون SLA.
    - Reservation pool of resources: نظام حجز الموارد المسبقة كنظام باقات بنسب مئوية بحيث تضمن توفر الموارد المطلوبة بالحدود القصوى وبكافة الأوقات وتحقق الجودة وفق الاتفاقية الموقعة مع الزبون SLA.
    - Flex allocation model: طريقة تجميع مرنة بحيث تضمن الجودة وتوفر في الاستهلاك فهي مزيج من الأنماط الثلاثة معاً وفق سياسات يتفق عليها مع الزبون في الاتفاقية الموقعة SLA.
17. أن تدعم المنظومة طريقة عمل الحاويات (containers) وإمكانية إدارتها وتحقيق الحماية لها بشكل عنقودي بطريقة سهلة وعن طريق واجهات سهلة الاستخدام أو عن طريق GUI/API/CLI.
18. أن توفر المنظومة إمكانية إنشاء ورفع ومشاركة تطبيقات معرفة ومعدة مسبقاً ضمن المنظمة بمختلف غرف البيانات الافتراضية وإمكانية مشاركة هذه التطبيقات بين المنظمات حسب الحاجة وبالتالي توفير الوقت والجهد.

19. أن توفر المنظومة إمكانية الوصول إلى التطبيقات والبرامج واستخدامهم من SaaS catalog وقت الحاجة ودون الحاجة إلى معرفة البنية التحتية بالإضافة إلى إمكانية تعديل الموارد المستهلكة بوقت قليل جداً (عدة ضغطات 1- click app deployment).
20. أن توفر المنظومة للزبون إمكانية إدارتها بشكل برمجي infrastructure as a code عن طريق استخدام الأنظمة العالمية المتعارف عليها مثل .../Terraform provider/Ansible وبالتالي إمكانية أتمتة أي عملية برمجية ضمن المنظومة أو على مستوى منظمة أو غرفة بيانات افتراضية.
21. يجب أن توفر المنظومة نافذة تمكن الزبون/المنظمة من رؤية معلومات الاستهلاك الخاصة بها على مستوى كامل الهيئة (المنظمة) أو على مستوى غرف البيانات الافتراضية أو على مستوى تطبيقات معينة بالإضافة إلى إمكانية رؤية معلومات الاستهلاك والفوترة على مستوى كافة المنظمات عن طريق مزود الخدمة.
22. أن توفر المنظومة لمزود الخدمة القدرة على معرفة إحصائيات حول المنظمات الأكثر استخداماً والأقل ربحاً وعن طرق تحسين الخدمة بما يضمن جني عائدات وأرباح أكثر مع ضمان جودة الخدمة بالإضافة إلى إمكانية توليد تقارير حسب الحاجة والطلب.
23. أن تقدم المنظومة القدرة على إعطاء خدمات الشبكة لكل منظمة على حدا مثل: Firewall Rules / Routing / NAT / DNS / DHCP / IDS/IPS.....
24. أن تدعم المنظومة عملية فصل المنظمات عن بعضها بحيث تضمن الجودة لكل منظمة وفق الاتفاقية الموقعة معها مع إمكانية تخصيص وتعريف واجهات وشعار لكل منظمة ووفق طلبها.
25. أن تدعم المنظومة عدة مصادر تحقق من الهوية (Authentication)متضمنة AD / LDAP / ADFS / SAML 2.0.
26. أن تدعم المنظومة طريقة Multi-tenant/ Multi-sites حيث أن الموارد قد تكون موجودة في مكان فزيائي واحد أو موزعة على عدة مواقع جغرافية موصولة معاً مع إمكانية عمل Tiering مع مستوى compute / storage / network.
27. يجب أن تكون المنظومة المستخدمة ذات بنية عنقودية بحيث تحقق الحماية العالية والأداء والجودة بالإضافة إلى إمكانية تحمل الضغط العالي في العمل والطلبات وأن تكون سهلة الاستخدام ومرنة ويمكن دمجها مع منظومات العمل الاخرى بسهولة وسرعة وألا تكون معقدة من حيث التركيب والصيانة والأعمال اليومية الإدارية والفنية وأن تحتفظ بمعلومات الاستخدام لفترات طويلة وإمكانية توليد التقارير حسب الحاجة وعند الطلب.
28. يجب أن تكون المنظومة ذات تقييم عالي وأن تكون معروفة عالمياً ومعترف بها.
29. يجب أن توفر المنظومة الجهد في إنجاز الأعمال التقنية اليومية والروتينية بالإضافة إلى توفير في الجهد والتكلفة مع إمكانية عمل تحديث لها ولكافة مكوناتها دون الحاجة إلى التوقف وضمان العمل خلال أعمال الصيانة الدورية.
30. يجب أن تكون المنظومة متكاملة وتضمن سلامة البيانات والإعدادات وإمكانية التعافي من الكوارث بسرعة مع إمكانية عمل نسخ احتياطية عن المنظومة ومكوناتها.

31. يجب أن تقدم المنظومة المستخدمة إمكانية بناء بنية سحابية محمية مما يحسن من فعالية غرف البيانات الافتراضية في توصيل الموارد من خلال تجميع CPU/RAM/Network/Storage وتقديمها بطريقة Catalog-based services وبالتالي استهلاك واستخدام الموارد بطريقة فعالة ومن دون مجهود وبطريقة مؤتمتة ومبرمجة وفق المعايير التي يحددها مدير المنظومة وإمكانية تقسيمها إلى فئات اعتماداً على نوعية الموارد، قدرة الموارد، حجم الموارد، أداؤها ومكان تمركزها.
32. إمكانية مشاركة الموارد والتطبيقات بين المبرمجين لتسريع عمليات التحديث والتطوير بالإضافة إلى إمكانية تطويرها بشكل برمجي حسب الحاجة ومتطلبات العمل.
33. إعطاء المنظمة إمكانية إدارة غرف بياناتها الافتراضية الخاصة بها بالإضافة إلى إدارة غرف البيانات الافتراضية المقدمة من المنظومة من مكان مركزي واحد.
34. يجب أن تكون المنظومة تدعم عمليات التشفير حسب طلب المنظمة المالكة للبيانات Encryption
35. يجب أن تتوفر لديه القدرات التالية:
    - يمكن ربطه حتى 30 مدير مراكز بيانات افتراضية في مناطق جغرافية مختلفة.
    - يمكن أن يضم ما يصل حتى 50000 مستخدم.
    - يمكن أن يضم 10000 منظمة وكل منظمة ممكن أن تضم:
        - 5000 مستخدم.
        - 5000 قالب برمجي.
        - 1000 شبكة.
        - 5000 مخدم افتراضي.
    - يمكن أن يصل عدد مراكز البيانات الافتراضية الى 10000 لكافة المنظمات.
    - يمكن أن يصل عدد الأقراص التخزين المستقلة حتى 10000.
    - عدد مخدمات افتراضية يصل حتى 40000.
    - عدد شبكات داخلية وخارجية يصل حتى 10000.
    - عدد مكونات مدراء شبكة برمجية 25.
    - عدد موجهات شبكية يصل حتى 10000.

5.1.2.2. مكون مراقبة الأحداث (*Log management system*)

هو المكون البرمجي ضمن البنية السحابية المسؤول عن إدارة سجلات الأحداث الناتجة عن كافة مكونات البنية السحابية في مكان مركزي مع إمكانية فرز هذه السجلات وفق تصنيفات تلائم بيئة العمل وعرضها بطريقة متطورة تساعد في تسهيل عمليات الدعم الفني وحل المشاكل التقنية والفنية.

يقوم هذا المكون بتجميع السجلات (Logs) من كافة المكونات الفيزيائية والافتراضية وتخزينها في قاعدة بيانات خاصة به ثم تحليل هذه المكونات وفق خوارزميات متطورة بحيث يمكن رؤية تقارير وتفاصيل أدق الأحداث التي تتم في المنظومة بطريقة انسيابية وسهلة باستخدام واجهات ومخططات ومع إمكانية توليده لإشعارات وتنبيهات ترسل إلى المسؤولين عن البنية عند الحاجة وفي حال ربطه مع مكون برمجي خاص بالأتمتة Workflow engine فإنه يمكنه تنفيذ أحداث وإجرائيات معرفة مسبقاً بطريقة مؤتمتة.

يعتبر هذا المكون من المكونات الأساسية في حل المشاكل الفنية والتقنية حيث يكون لديه واجهات تحليلية بطرق تفاعلية تبسط وتسهل عملية حل المشاكل وفهم الأحداث المترابطة معاً.

<u>يجب أن تتوفر في هذا المكون الشروط الفنية التالية:</u>

1. يجب أن يكون مبني بطريقة عنقودية (Cluster) بحيث تلغي وجود نقطة فشل وحيدة فيه وتضمن استمرار عمله وأداء مهامه.
2. إمكانية برمجته بطريقة مؤتمتة وأن يدعم REST API.
3. يجب أن يحتوي المكون على واجهات تفاعلية لعرض السجلات والأحداث.
4. إمكانية تخصيص الواجهات (Dashboard) والمخططات والتنبيهات والإشعارات حسب الحاجة.
5. إرسال التقارير الدورية والإشعارات والتنبيهات بعدة طرق الى المسؤولين عن المنظومة.
6. عملية جمع السجلات بطريقة مؤمنة ومشفرة بينه وبين باقي العناصر والمكونات.
7. أن يدعم إعطاء الصلاحيات للمستخدمين حسب مهامهم Role-Based Access Control.
8. إمكانية مشاركة الواجهات (Dashboard) بين المستخدمين.
9. عمل أعمار زمنية للسجلات (Log Retention) مع إمكانية الأرشفة والتصدير الى مكان أخر.

5.1.2.3. مكون مراقبة الأداء والعمليات

يسهل عمليات فريق الدعم الفني (IT) في حل المشاكل ومراقبة كافة المكونات بطريقة عصرية مؤتمتة حيث يمكن الفريق من مراقبة المكونات والموارد الموجودة في مراكز البيانات الافتراضية الموجودة محلياً أو الموجودة في مركز البيانات الافتراضية الموجودة ضمن البنية السحابية.

تتمدد البنى التحتية ضمن البنية السحابية وتتوسع بسرعة لأنها مؤتمتة وتكون متاحة عند الطلب، بالإضافة الى أن موارد البنية التحتية ممكن أن تكون موزعة على أكثر من مكان فيزيائي ومستخدمة من عدة منظمات تختلف في متطلباتها الفنية والتقنية، وبالتالي يمكن من خلال هذا المكون رؤية كافة الموارد الافتراضية والفيزيائية في البيئة وطريقة استخدامها من كل تطبيق برمجي موجود في البنية، بالإضافة إلى عرض الإحصائيات الخاصة بالاستخدام من قبل كل مخدم افتراضي، وعلى كل مكون فيزيائي سواء كان شبكة أو موارد تخزين أو موارد معالجة.

من خلال هذا المكون ضمن البنية السحابية يمكن لكل منظمة وهيئة رؤية إحصائيات الاستخدام للموارد التشغيلية الخاصة بهم على المخدمات الافتراضية وضمن الشبكات الخاصة بهم وعلى كافة موارد التخزين الخاصة بهم، بالإضافة إلى رؤية الموارد غير الضرورية والاستغناء عنها، بالإضافة إلى الموارد التي يجب زيادتها للحصول على الأداء الأمثل المحتاج. كما يمكن رؤية الإعدادات التي يجب تعديلها لوجود أخطاء تشغيلية كما يقدم الاقتراحات الأمثل المناسبة لكل تطبيق برمجي موجود ضمن مركز البيانات الافتراضية الخاصة بها.

يمكن لكل منظمة وهيئة من خلال هذا المكون ضمن البنية السحابية توليد تقارير تشغيلية تخص كل تطبيق برمجي موجود لديهم وكل مخدم افتراضي وكل مكون شبكي وكل مكون تخزيني، مع إعطاء تقارير تخص كمية الموارد التي سيكونون بحاجة لها بعد عدة أشهر أو عدة سنين أو حسب مدة زمنية يتم تحديدها من قبل مسؤول الهيئة/المنظمة.

تكون التطبيقات ضمن البنية السحابية مقدمة إما بطريقة تقليدية عن طريق تنصيبها على مخدمات افتراضية ضمن مراكز البيانات الافتراضية أو تكون مقدمة بالطريقة العصرية الحديثة المعروفة بالحاويات البرمجية (Containers) والتي تتم إدارتها عن طريق مكون برمجي يعرف بالقبطان (Kubernetes).

يقدم هذا المكون قدرة تحكم كاملة على كافة التطبيقات المركبة بطريقة تقليدية أو المعدة بطريقة مطورة بالإضافة إلى قدرة حل المشاكل التشغيلية المتعلقة بهم ورؤية خرائط تظهر طريقة عملهم وتموضعهم ضمن البنية السحابية والعلاقة بينهم وبين كل مكون برمجي وفيزيائي موجود ضمن البنية وكمية الموارد المستهلكة وعرض التوصيات والتحذيرات والاقتراحات حيث أن عملية استكشاف نوع التطبيقات التي تعمل وفرزهم حسب طبيعة عملهم هي عملية تلقائية ومؤتمتة.

<u>يجب أن تتوفر في هذا المكون الشروط الفنية التالية:</u>

1. يجب أن يكون مبني بطريقة عنقودية (Cluster) بحيث تلغي وجود نقطة فشل وحيدة فيه وتضمن استمرار عمله وأداء مهامه.
2. يجب أن يكون هذا المكون قابل للإعداد بطريقة برمجية باستخدام طريقة REST API.
3. يجب أن يكون قادر على مراقبة ما يصل حتى 10000 عميل (Agent).
4. أن يدعم إعطاء الصلاحيات للمستخدمين حسب مهامهم Role-Based Access Control.
5. يجب أن تكون الاتصالات بين المكون المركزي والعملاء (Agents) مشفرة وآمنة باستخدام SSL.

<u>الميزات التي يجب أن يقدمها هذا المكون الى مشغل خدمة البنية السحابية:</u>

1. الرؤية الكاملة والواضحة لكافة المكونات الموجودة ضمن البنية السحابية سواء كانت مكونات افتراضية أو فيزيائية وإظهار العلاقة بينهم بشكل خرائط لإزالة التعقيدات الناتجة عن وجود العدد الهائل من المكونات المتداخلة فيما بينها مع إظهار علامات على كل مكون موجود ضمن الخريطة تظهر حالته التشغيلية والتي تعكس ضمنياً حالة كل مكون مرتبط به.

2. سهولة حل المشاكل التشغيلية من خلال تجزئة كامل البنية إلى قطع صغيرة متناسقة مترابطة مع بعضها البعض بشكل خرائط هندسية تظهر أدق التفاصيل التشغيلية من حيث الأداء والتوصيات والإشعارات الخاصة بكل مكون برمجي وفيزيائي موجود ضمن المنظومة وعرض المكونات غير متناسقة مع السياسة والقوانين التشغيلية للبنية وتقييم أداء كل مكون بالإضافة إلى عرض التنبيهات التشغيلية التي قد تسبب مشاكل في المستقبل القريب بسبب أخطاء تشغيلية أو عدم تناغم وتناسق في الاعدادات الحالية.
3. سهولة البحث عن أي مكون ضمن البنية من خلال عدد كبير من المعايير مثل اسمه أو طريقة عمل أو تصنيفه أو الوسم الذي يملكه أو مكان تمركزه بالإضافة الى استخدام هذه المعايير في الفرز والتصنيف وعرض قوائم بأكثر المكونات فعالية أو الأكثر استهلاكا أو الأكثر نمواً.
4. إمكانية تخصيص الواجهات والقوائم والتقارير والتنبيهات والتحذيرات والتوصيات وإرسال تقارير تشغيلية بشكل دوري أو عند الحاجة أو عند حدوث أمر معين في المنظومة أو في أحد مكوناتها.
5. عمل إدارة ودراسة لموارد البنية الموجودة حاليا (Capacity Management) وتقييم طريقة استهلاكها خلال فترات زمنية معينة لإظهار وتوليد خطة التوسع المستقبلية (Capacity Plan).
6. استكشاف التطبيقات الموجودة حالياً وفرزها في مجموعات حسب طبيعة عمل كل منهم بالإضافة إلى عرض أدق التفاصيل التشغيلية من حيث الأداء والاستهلاك وإظهار كمية الموارد التشغيلية المطلوبة بدقة في كافة أوقات العمل بالإضافة إلى عرض الموارد المحجوزة وغير المستخدمة مع إمكانية توليد تقارير واقتراحات حول أفضل مكان لتواجد هذه التطبيقات.
7. عمل تناغم وترشيد استهلاك على مستوى البنية كاملة حيث يريك التوصيات التي تحسن في أداء واستهلاك الموارد على مستوى غرف البيانات المركزية الفيزيائية أو غرف مراكز البيانات الافتراضية أو على مستوى المخدمات وأجهزة التخزين والمكونات الشبكية أو على مستوى البنى العنقودية.
8. دعم استخدام سيناريوهات ماذا-لو (What-if Analysis) حيث تمكن من عمل محاكاة لأي تعديل في البنية بحيث تظهر الفوائد والحسنات والسيئات الناتجة عن تنفيذ هذا التعديل وتأثيره على كامل المنظومة ومكوناتها.

5.1.2.4. مكون الأتمتة

هو المكون البرمجي (Workflow engine) ضمن البنية السحابية الذي يسهّل ويؤتمت عمليات الدعم الفني (IT) في انجاز عمليات الدعم الفني (IT Operation) المعقدة. حيث يمكن الترابط والتناغم مع باقي المكونات البرمجية الموجودة في البنية السحابية لتنفيذ السكريبتات والعمليات المؤتمتة (Workflows) عند الضرورة أو وفق جداول زمنية معينة.

الفائدة الرئيسية لهذا المكون هي إمكانية تنفيذ أي عملية مهما كانت معقدة بسهولة (مثل تخصيص عناوين IP من نظام إدارة مركزي أو إضافة مستخدمين ومجموعات إلى مدير الحسابات أو إنجاز الإجرائيات الملائمة لكل تنبيه وتحذير يحدث في المنظومة أو تحديث قاعدة بيانات معينة أو حتى انشاء وإعداد مكون برمجي مثل موزع أحمال (Load Balancer) أو عمل نسخ احتياطية

عن أنظمة معينة وفق شروط معينة أو ...الخ) عن طريق استخدام Workflow الملائم لإنجاز هذه المهمة مع العلم أنه توجد مكتبة ضخمة من Workflows الجاهزة للاستخدام الفوري دون الحاجة لأي تعديل مع إمكانية كتابة Workflow جديد أو تعديل Workflow موجود بسهولة وسرعة ودون الحاجة إلى خبرات متقدمة في كتابة Workflow.

يمكن من خلال هذا المكون كتابة سكريبت برمجي حيث يمتلك هذا المكون محرك سكريبتات برمجية مطورة يدعم:

1. version control
2. variable type checking
3. namespace management
4. Exception Handling

مع إمكانية صنع كتل برمجية مكونة من: Actions & Workflow & Policies ويدعم عدة لغات برمجية عالمية مشهورة مثل: PowerShell / Node.js / Python وكافة Workflows لديها قدرات وميزات مثل: / Version history Packaging / Rollback

يمكن ربط ودمج هذا المكون مع أدوات التحكم الخاص بالبنية السحابية مما يمكّن من توسيع قدراتهم وإمكانياتها في إدارة البنية السحابية والمرونة في الاستجابة الى أي تغيرات ومتطلبات في العمل التي تنمو وتتطور باستمرار نتيجة لطبيعة عمل البنية السحابية التي تلبي متطلبات كافة مستخدميها على الرقم من اختلاف طبيعة عملهم واحتياجاتهم.

<u>الميزات الواجب توفرها في المكون:</u>

1. يجب أن يكون مبني بطريقة عنقودية (Cluster) بحيث تلغي وجود نقطة فشل وحيدة فيه وتضمن استمرار عمله وأداء مهامه.
2. يجب أن يكون هذا المكون قابل للإعداد بطريقة برمجية باستخدام طريقة REST API.
3. أن يدعم إعطاء الصلاحيات للمستخدمين حسب مهامهم Role-Based Access Control.

5.1.2.5. مكون نظام الفوترة

هو المكون البرمجي ضمن البنية السحابية المسؤول عن عمليات التسعير وإدارة الأعمال والتكاليف التشغيلية حيث أنه يقوم بتوليد تقارير لحظية عند الطلب حول تكلفة كل عنصر من العناصر الموجودة ضمن البنية السحابية سواء كانت فيزيائية أو افتراضية كما يمكن حساب التكاليف التشغيلية وفق فترات زمنية معينة بالإضافة الى إظهار تكاليف الصيانة وإعطاء تقارير مالية.

يمكن للمسؤولين والمستخدمين منظمات وأفراد ضمن البنية السحابية رؤية التكاليف المالية الخاصة بهم قبل طلب الخدمة أو خلال طلب الخدمة كما يمكنهم رؤية التكاليف التشغيلية الخاصة بهم لاحقاً ومعرفة حجم الاستهلاك والإنفاق لكل تطبيق وخدمة يستفيدون منها. كما يمكن لهؤلاء المستخدمين والأفراد من رؤية طرق ترشيد الإنفاق والتكاليف مثل نقل تطبيقاتهم من مكان

فيزيائي لآخر أو نقلهم من مخدمات عالية التكاليف والتصنيف إلى مخدمات أقل كلفة أو تغير نوع وحدات التخزين إلى وحدات تخزين أقل كلفة وأقل أداء وغيره من الأمور التي تساعدهم على عمل توازن بين الخدمة والتكاليف.

يستطيع مزودو البنية السحابية من خلال هذا المكون تقييم الاستثمار الموضوع في البنية من كافة الجوانب الفنية واللوجستية وتحديد مقدار الاستفادة المالية من الخدمات المقدمة وماهي أكثر المنظمات والأفراد المستهلكة وطبيعة استهلاكهم بحيث يمكنهم التركيز على طرق تحسين الجودة وتحديد أفضل الخدمات التي تعيد عائدات مالية. كما يمكن لمزود الخدمة أن يقوم بالتسعير حسب المكان الفيزيائي حيث تقدم الخدمة أو حسب نوع المعدات الفيزيائية المستخدمة لتلبية هذه الخدمة. بالإضافة الى إمكانية عمل سياسات نقدية ومالية وتوليد التقارير الفنية والمالية حسب الطلب والحاجة.

الميزات الواجب توفرها في المكون:

1. يجب أن يكون مبني بطريقة عنقودية (Cluster) بحيث تلغي وجود نقطة فشل وحيدة فيه وتضمن استمرار عمله وأداء مهامه.
2. يجب أن يكون هذا المكون قابل للإعداد بطريقة برمجية باستخدام طريقة REST API.
3. أن يدعم إعطاء الصلاحيات للمستخدمين حسب مهامهم Role-Based Access Control.

5.1.2.6. مكون الحماية والإتاحة

هو المكون البرمجي ضمن البنية السحابية المسؤول عن عمليات النسخ الاحتياطية والاسترجاع البيانات عند الحاجة (Backup and Restore) مع إمكانية عمل أكثر من نسخة من البيانات (Replication) في أكثر من موقع فيزيائي وعلى أكثر من وحدة تخزين مركزية مختلفة (SAN/NAS/vSAN).

يمكن للمسؤولين والمستخدمين منظمات وأفراد ضمن البنية السحابية القيام بوضع سياسات حماية بخصوص النسخ الاحتياطية والاسترجاع والمزامنة لكل تطبيق خاص بهم وعمل جدولة لهذه السياسات ورؤية حالة تنفيذ هذه السياسات ومن يطبعها ومن يتخلّف عن تطبيق هذه السياسات وكل ذلك من مكان مركزي واحد وبطريقة سهلة (GUI) ولا تحتاج الى خبرات فنية خاصة. كما يمكنهم القيام بصنع نسخ احتياطية لبيانات وملفات معينة وليس لكامل المخدم الافتراضي. كما يمكنهم من مكان مركزي رؤية حالة عمليات النسخ الاحتياطي والمزامنة والاسترجاع الناجحة منهم والفاشلة وسبب فشلها أو توقفها.

يستطيع مزودي البنية السحابية من خلال هذا المكون تقديم واحدة من أهم الخدمات بالنسبة للزبائن وهي تأمين البنية التحتية لعمليات النسخ الاحتياطي والاسترجاع والتي تؤمن للزبائن والمستهلكين حماية البيانات ومن ناحية أخرى فإن مزودي الخدمة يستخدمون هذا المكون لحماية بياناتهم والإعدادات الخاصة بكل مكون موجود في البنية بالإضافة إلى عمل نسخ احتياطية عن كامل مراكز البيانات الافتراضية التي لديهم وتوفير إمكانية عمل سياسات حماية مختلفة تلائم كافة المتطلبات.

الميزات الواجب توفرها في المكون:

1. يجب أن يكون مبني بطريقة عنقودية (Cluster) بحيث تلغي وجود نقطة فشل وحيدة فيه وتضمن استمرار عمله وأداء مهامه.
2. يجب أن يكون هذا المكون قابل للإعداد بطريقة برمجية باستخدام طريقة REST API.
3. أن يدعم إعطاء الصلاحيات للمستخدمين حسب مهامهم Role-Based Access Control.

5.1.3. إدارة معلومات الحماية وأحداث الحماية (*SIEM*)

هو نظام إدارة للحماية موحّد يقدم رؤية واضحة لكل نشاطات الشبكة ويمكّن المستخدم من الرد على التهديدات في الوقت الحقيقي. يقوم بجمع بيانات الآلات من مصادر متنوعة ويقوم بتصنيفها في مجموعات ومن ثم يقوم بتحليلها لتقديم ما يلزم من البيانات المحللة لاتخاذ قرار.

يقوم هذا الحل البرمجي بالبحث في كمية ضخمة من البيانات خلال ثواني للعثور والتنبيه إلى وجود سلوك غير طبيعي (unusual behavior) في البيئة مما يقدم رؤية واضحة للبيئة في الوقت الحقيقي في الوقت الحقيقي وهذه مهمة مستحيل القيام بها بشكل يدوي.

بكلمات أخرى، يقدم هذا الحل البرمجي لمحة (snapshot) عن البيئة من دون توقيف عمليات التخزين وعمليات السجل (log) وتسمح إمكانية تحليل هذه البيانات الضخمة لفريق IT ليس فقط بالقيام بالرد على التهديدات بل تسمح بكشف نقاط الضعف وبالتالي العمل على حلها قبل حدوث أي اختراق أمني.

يجمع هذا الحل البرمجي إدارة أحداث الحماية (SEM) التي تقوم بتحليل السجلات وبيانات الأحداث في الوقت الحقيقي لتقديم إمكانية مراقبة التهديدات وتجميع الأحداث والاستجابة للأحداث مع إدارة معلومات الحماية (SIM) التي تجمع وتحلل وتقدم تقارير من بيانات السجلات.

كيفية عمل SIEM:

يقوم هذا الحل البرمجي بتجميع بيانات الأحداث من مصادر مختلفة داخل البنية الشبكية ويتضمن ذلك المخدمات والأنظمة والأجهزة والتطبيقات. يقوم هذا الحل البرمجي بشكل أساسي بتقديم معلومات ذات سياق حول المستخدمين والموارد المهمة (assets) وغير ذلك. يقوم بتجميع وتحليل البيانات لفحص وجود انحرافات او اختلافات عن السلوك الطبيعي ويقارنها بمجموعة من القواعد لتعريف التهديدات التي من الممكن حدوثها.

تتضمن مصادر البيانات:

1. أجهزة الشبكة: موجهات (Routers) – موزعات (Switches) – الجسور (bridges) نقاط الوصول اللاسلكية – hubs – line drivers
2. المخدمات: web – proxy – mail – FTP
3. أجهزة الحماية: IDS/IPS – الجدران النارية – برامج مضاد الفيروسات – أجهزة فلترة المحتوى – أجهزة كشف الاختراقات (Intrusion detection appliance)
4. التطبيقات: أي نظام برمجي يتم استخدامه على أي من الأجهزة المذكورة سابقاً.

تتضمن الخصائص التي يمكن تحليلها: المستخدمين وأنواع الأحداث وعناوين IP والذاكرة والمهام (processes) وغيرها...

يقوم هذا الحل البرمجي بتصنيف الانحرافات (deviations) كمحاولة ولوج فاشلة أو تغيير في الحساب الشخصي أو برنامج خبيث محتمل أو...

عند حدوث أي انحراف يقوم الحل البرمجي بإرسال تنبيه إلى المسؤول عن الحماية وقد يتوقف هنا عن العمل ولكن يمكنه أيضاً أن يقوم بتعليق النشاط غير الطبيعي. يقوم المسؤول عن هذا الحل البرمجي بتحديد ماهي الأحداث التي تؤدي إلى إرسال تنبيه وما الإجراءات التي يلزم اتخاذها عند التعامل مع نشاط خبيث مشتبه به.

ينتبه هذا الحل البرمجي للأنماط والتصرفات الشاذة (anomalous behavior) وبالتالي إذا لم يؤدي إلى حدوث تنبيه فإن الحل البرمجي سيقوم بكشف الترابط بين عدة أحداث وسيقوم عندها بإرسال تنبيه وكشف التصرف الشاذ.

يقوم هذا الحل البرمجي بتخزين تلك السجلات في قاعدة البيانات مما يسمح للمسؤول عن هذا الحل البرمجي بالقيام بإجراء تحقيقات أعمق.

وبالتالي فإن هذا الحل البرمجي يقدم إمكانيات إدارة السجل الأساسية مع إمكانية إرسال التنبيهات ولوحات التحكم التفاعلية وتعلم الآلة (machine learning) والقدرة على البحث في البيانات التاريخية من أجل التحليل.

عندما يقوم الحل البرمجي بتعريف نشاط معين على أنه تهديد يتم توليد إنذارات لتحذر من وجود مشكلة محتملة في الحماية. ويتم تحديد مستوى أهمية الإنذار.

يوجد هدفين رئيسيين لهذا المكون البرمجي:

1. تقديم تقارير عن الحوادث والأحداث المتعلقة بالحماية مثل محاولات تسجيل الدخول الناجحة والفاشلة ونشاطات البرمجيات الخبيثة (malware) وأي نشاطات خبيثة محتملة.
2. إرسال إنذارات إذا كان التحليل يظهر أن حدث معين تم مقارنته بمجموعة من القواعد وتبين أنه توجد مشكلة محتملة في حماية المنظومة.

الميزات الواجب توفرها في المكون:

1. **المراقبة في الوقت الحقيقي:** يجب أن يقدم هذا الحل البرمجي ملخص عن كل ما يحدث في الشبكة في الوقت الحقيقي ويتضمن ذلك النشاطات المرتبطة بالمستخدمين والأجهزة والتطبيقات والنشاطات غير المرتبطة بهوية (identity) بشكل خاص. يجب أن يحتوي هذا الحل البرمجي على القدرة على صياغة تلك المعلومات بصيغة قابلة للاستخدام. يجب أن يحتوي على مكتبة من قواعد الارتباط المعرفة مسبقاً والقابلة للتخصيص. يجب أن يحتوي على واجهة (console) لأحداث الحماية لتقديم عرض في الوقت الحقيقي لحوادث الحماية (security incidents) وأحداث الحماية (security events) ولوحات تحكم لتقديم عرض مباشر (live) لنشاطات التهديدات.
2. **الاستجابة للحوادث (Incident Response):** يجب أن يملك هذا الحل البرمجي القدرة على الاستجابة التلقائية لمقاطعة الهجمات أثناء حدوثها. يجب أن يملك القدرة على تعريف الأحداث الجديرة بالذكر وحالاتها والتأشير إلى مدى خطورتها والبدء بمعالجة هذه المشاكل وتقديم تقرير (audit) لعملية المعالجة المتعلقة بحادثة معينة بأكملها.
3. **مراقبة المستخدمين:** قد تكون بعض التهديدات داخلية إما لأن المستخدمين يشكلون خطراً حقيقياً أو لأن تصرفاتهم تعرّض البيئة لتهديدات خارجية. يجب أن يقدم هذا الحل البرمجي القدرة على تحليل بيانات الوصول والتوثيق (authentication) ويشكّل سياق للمستخدم (user context) وتقديم تنبيهات (alerts) فيما يتعلق بالتصرفات المشبوهة وانتهاكات للسياسات التنظيمية.
4. **تقصي معلومات متعلقة بالتهديدات (Threat Intelligence):** يجب أن يستطيع هذا الحل البرمجي أن يساعد مدير النظام في تعريف التهديدات الخارجية الرئيسية أو المعروفة بـ zero-day exploits والتهديدات المتقدمة والمستمرة (persistent). تستطيع هذا الميزة أن تقدم القدرة على تعريف النشاطات غير الطبيعية وتعريف نقاط الضعف في البيئة قبل أن يتم استغلالها وتشكيل استجابات وطرق معالجة لنقاط الضعف تلك.
5. **التحليل المتقدم وتعلم الآلة (machine learning):** توظّف ميزة التحليل المتقدم أساليب كميّة متطورة مثل الإحصائيات والتنقيب عن البيانات (data mining) الوصفي والتنبؤي والمحاكاة والتحسين لتقديم نظرة أعمق. إن الحلول البرمجية التي تستخدم تعلم الآلة (machine learning) قادرة على تتعلم مع مرور الوقت ما يمثل التصرفات الطبيعية وما هو انزياح حقيقي عن التصرفات الطبيعية مما يحسن دقة النتائج.
6. **الكشف التهديدات المتقدم (Advanced Threat Protection):** يجب أن يستطيع هذا الحل البرمجي القيام بمزيج من مراقبة حماية الشبكة والكشف عن الأجهزة (endpoint detection) وتجريب الاستجابة في بيئة اختبار منعزلة (response sandboxing) وتحليل التصرفات لتعريف وحجر التهديدات الجديدة. فهذه الميزة لا تقدم فقط الكشف عن التهديد بل استيعاب مدى خطورته وإلى أين يتحرك بعد اكتشافه وكيفية احتوائه.
7. إدارة سلسة للسجلات: يجب أن يستطيع هذا الحل البرمجي أن يجمع بيانات من مئات وآلاف من المصادر ويجب أن يقدم واجهة سهلة الاستخدام يمكن استخدامها لإدارة والحصول على بيانات السجل.
8. إعطاء فريق IT وقتاً للاستجابة عند حدوث محاولة اختراق.
9. منع الهجمات المحتمل حدوثها.

10. تقليل تأثير محاولات اختراق المنظومة إن حدثت.
11. زيادة فعالية المنظومة.
12. بما أن هذا الحل البرمجي في صلبه هو نظام تجميع بيانات ونظام بحث ومولّد تقارير فهو يستطيع أن يجمع كميات ضخمة من البيانات من كامل المنظومة ومن ثم تجميعها وتحليلها وجعلها سهلة الاستيعاب ومن ثم يقدمها في واجهة واحدة مركزية يستطيع مدير المنظومة من خلالها أن يرى كل ما يحدث داخل منظومته.

<u>لوحات التحكم المطلوبة:</u>

1. ملخص عن الأحداث الجديرة بالذكر في البيئة والتي تمثل أحداث حماية محتملة.
2. تفاصيل عن الأحداث الجديرة بالذكر: يستطيع المسؤول عن النظام أن يقوم بعملية الفرز وتحديد مدى خطورة كل حدث.
3. جميع التحقيقات التي تجري حالياً مما يسمح للمسؤول عن النظام بالتحقق من مدى تقدمه بينما يقوم بالتحري في أكثر من حادثة متعلقة بالحماية.
4. تحليل المخاطر لفحص الأنظمة والمستخدمين عبر الشبكة لتعريف المخاطر.
5. تقصي معلومات متعلقة بالتهديدات (Threat Intelligence): المصمم لإضافة سياق إلى حوادث الحماية ولتعريف المستخدمين الخبيثين (malicious actors) في البيئة.
6. تقصي معلومات متعلقة بالبروتوكولات (Protocol Intelligence): باستخدام طرود البيانات التي تم التقاطها لتقديم معرفة متعلقة بالشبكة ذات صلة بتحقيقات الحماية مما يسمح للمسؤول عن النظام بتعريف البيانات (traffic) المشبوهة ونشاطات DNs المشبوهة ونشاطات البريد الإلكتروني المشبوهة.
7. تقصي معلومات متعلقة بالمستخدمين (User Intelligence): يسمح للمسؤول عن الحل البرمجي بمراقبة والتحقيق في نشاطات المستخدمين والموارد الهامة (assets) في البيئة.
8. تقصي معلومات متعلقة بحركة الويب (Web intelligence): لتحليل حركة الويب في الشبكة.

5.2. التجهيزات العتادية المطلوبة

5.2.1. جدول الكميات للتجهيزات المطلوبة

#	الوصف	العدد
1	مخدم	5
2	مبدل switch (10G)	4
3	مبدل L3 (1G) switch	4
4	Next Generation Firewall	2
5	NAS Storage	1
6	قطع تبديل وتوسعة للمخدمات	

5.2.2. المواصفات الفنية للمخدمات (عدد 5)

#	شرط رفض	اسم المواصفة	المواصفة الفنيّة المطلوبة
1		الماركة	- من إنتاج إحدى الشركات العالمية المتخصصة في هذا المجال والمعروفة بجودة منتجاتها العالية في السوق العالمية. - يطلب من العارض تحديد الماركة بشكل صريح وواضح.
2		الطراز	- يطلب من العارض تحديد الطراز بشكل صريح وواضح. - يجب أن تكون المخدمات المقدمة من أحدث الطرازات المنتجة من الشركة المصنعة.
3		بلد المنشأ/الصنع	يطلب من العارض تحديد بلد المنشأ وبلد الصنع بشكل صريح وواضح.
4		الشكل Form Factor	2U Rack Max
5		اللوحة الرئيسية	Intel C621 Chipset

#	شرط رفض	اسم المواصفة	المواصفة الفنيّة المطلوبة	
6	شرط رفض	المعالج processor	الماركة Brand:	Intel Xeon Gold Processor
			الطراز Model:	يطلب من العارض تحديد الطراز بشكل واضح وصريح
			عدد وحدات المعالجة المطلوبة:	2 Processors with high performance Heatsink
			عدد النوى في كل وحدة Core:	24 core على الأقل
			السرعة CPU Frequency:	2.0 GHz على الأقل
			الذاكرة المخبئية L3 Cache:	25 MB على الأقل
7	شرط رفض	الذّاكرة الرّئيسية memory	السعة العظمى Maximum Capacity:	24 DIMM Available (12 DIMM Per Processor)
			السعة المطلوبة Capacity:	512 GB (16*32 GB)
			النوع Type:	RDIMM – Dual Rank x4 DDR4
			السرعة:	2666 MHz على الأقل
8	شرط رفض	الأقراص الصلبة HDD	وحدات التخزين المطلوبة:	- 2 HDD SAS 300GB - 6 SSD 2TB
			بطاقة التحكم بالأقراص الصلبة Storage Controller:	- Smart Array P4081-a SR Gen10 Controller (8 Internal Lanes/2GB Cache)

#	شرط رفض	اسم المواصفة	المواصفة الفنيّة المطلوبة	
			- Storage Battery Included	
			- RAID Controller Support for RAID Level 0,1,5,6	RAID Support
9		بطاقة الشّبكة Network Card	- 4* 1G - 2* 10G	عدد المنافذ – السرعة
10		المراوح الداخلية	6*Redundant Fan High Performance	
11	شرط رفض	التّغذية الكهربائيّة Power supply	2 Redundant hot-plug AC power supply Low Halogen	
			الاستطاعة: W800	
12		السواقة الليزرية	SATA DVD R/W Optical Drive	
13		المنافذ :Interfaces	- 5 USB 3.0 (1front – 2 Rear – 2 Internal) - 1 Micro SD Internal Slot - Front Display Port - VGA Display Port - iLO Front Service Port - 1GB dedicated iLO Remote Management Network Port	
14		Front Panel LEDs	- System Power LED - Health LED - NIC Status LED - SID Systems Insight Display LEDs (processor LEDs – DIMM LEDs – FAN LEDs – NIC LEDs – Power Supply LEDs – Over Temp LED	

#	شرط رفض	اسم المواصفة	المواصفة الفنيّة المطلوبة
15		متوافق مع أنظمة التّشغيل	Operating Systems and Virtualization Software Supported: - Microsoft windows server 2012 -2016 - Red Hat enterprise Linux (RHEL) 6.9 and 7.3 - VMware ESXI 6.0 – 7.1 - CentOS - Ubuntu
16		الكبلات المطلوبة	- 2 * European Power Cord - 4 * Ethernet Cable 5m CAT 6 Patch Cord RJ45
17		guarantee	Not less than a full Gregorian year

5.2.3. المواصفات الفنية لمبدل *(switch) 1G* عدد 4

#	شرط رفض	اسم المواصفة	المواصفة الفنية المطلوبة
1		الماركة والطراز	- من إنتاج إحدى الشركات العالمية المتخصصة في هذا المجال والمعروفة بجودة منتجاتها العالية في السوق العالمية. - يطلب من العارض تحديد الماركة والطراز
2	شرط رفض	Product	10/100/1000 Rj-45 copper ports
3	شرط رفض	Number of Ports	24 x 10/100/1000
4	شرط رفض	RAM	4 GB
5	شرط رفض	Flash Memory	2 GB
6	شرط رفض	Performance	– Switching capacity: 88 Gbps – Stacking bandwidth: 480 Gbps
7	شرط رفض	Capacity	– IPv4 routes: 24000

#	شرط رفض	اسم المواصفة	المواصفة الفنية المطلوبة
			– NetFlow entries: 24000 – Switched virtual interfaces (SVIs): 1000 – Manageable access points: 5
8		Routing Protocols	RIP-1, RIP-2, EIGRP, RIPng
9		Remote Management Protocols	SNMP 1, RMON 1, RMON 2, Telnet, SNMP 3, SNMP 2c, SSH, CLI
10		Features	Auto-negotiation, ARP support, trunking, VLAN support, auto-uplink (auto MDI/MDI-X), IGMP snooping, Syslog support, IPv6 support, Rapid Spanning Tree Protocol (RSTP) support, Multiple Spanning Tree Protocol (MSTP) support, DHCP snooping, Dynamic Trunking Protocol (DTP) support, Port Aggregation Protocol (PAgP) support, Trivial File Transfer Protocol (TFTP) support, Access Control List (ACL) support, Quality of Service (QoS), RADIUS support, Virtual Route Forwarding-Lite (VRF-Lite), MLD snooping, Dynamic ARP Inspection (DAI), PoE+, STP Root Guard, Uni-Directional Link Detection (UDLD), Rapid Per-VLAN Spanning Tree Plus (PVRST+), IPv4 support, Shaped Round Robin (SRR), Link Aggregation Control Protocol (LACP), Remote Switch Port Analyzer (RSPAN), layer 3 load balancing, Energy Efficient Ethernet, Cisco StackWise-480 technology, Cisco StackPower technology, Flexible NetFlow (FNF)
11		guarantee	Not less than a full Gregorian year

5.2.4. المواصفات الفنية لمبدل *10G (switch)* عدد 4

#	شرط رفض	اسم المواصفة	المواصفة الفنية المطلوبة
1		الماركة والطراز	- من إنتاج إحدى الشركات العالمية المتخصصة في هذا المجال والمعروفة بجودة منتجاتها العالية في السوق العالمية - يطلب من العارض تحديد الماركة والطراز
2	شرط رفض	Product	100M/1G/10G Rj-45 copper ports
3	شرط رفض	Number of Ports	(at least)24
4		USB PORTS	for config file upload / backup & firmware updates
5	شرط رفض	MEMORY	Packet buffer memory Dynamically shared across only used ports (2 MB at least)
6		Forwarding mods	Store-and-forward
7	شرط رفض	Bandwidth	160 Gbps at least
8		Multicast groups	512 at least
9		Number of Ipv4 static routes	32
10		Number of ARP cache entries	738 at least
11		Number of DHCP snooping bindings	8K at least
12		Access control lists (ACLs)	100 shared for MAC, IP ACLs

#	شرط رفض	اسم المواصفة	المواصفة الفنية المطلوبة
13		Packet forwarding rate	119.0 at least
14		IPv4 /IPv6 ACL and QoS	L2 , L3 , L4 ingress
15		Fabric	160Gbps (Line-rate) at least
16	شرط رفض	CPU	600 MHz Cortex-A9 Single Core, 512MB RAM (at least) 8MB SPI + 256MB NAND FLASH
17		guarantee	Not less than a full Gregorian year

5.2.5. المواصفات الفنية للجدار الناري (Next Generation Firewall) عدد 2

#	شرط رفض	اسم المواصفة	المواصفة الفنية المطلوبة
1		الماركة والطراز	- من إنتاج إحدى الشركات العالمية المتخصصة في هذا المجال والمعروفة بجودة منتجاتها العالية في السوق العالمية. - يطلب من العارض تحديد الماركة والطراز.
2	شرط رفض	Hard Drive	SSD
3	شرط رفض	Interfaces	At Least: - 6 x 1000Base-T - RJ-45 - 1 x serial - RJ-45 - 1 x USB 3.0 - Type A - 1 x micro-USB - 1 x HDMI - 2 x 1000Base-X - SFP (mini-GBIC)

#	شرط رفض	اسم المواصفة	المواصفة الفنية المطلوبة
6		Connectivity Technology	Wired
8	شرط رفض	Data Link Protocol	– Ethernet – Fast Ethernet – Gigabit Ethernet
9	شرط رفض	Performance	At Least: – Firewall throughput: 25 Gbps – VPN throughput: 1.45 Gbps – Intrusion prevention throughput: 4.0 Gbps – Antivirus throughput (proxy): 2.3 Gbps – NGFW throughput: 3.0 Gbps – Firewall throughput (IMIX): 5.5 Gbps – Threat Protection: 800 MBPS
10		Capacity	– Maximum number of users: unlimited – Concurrent connections: 8200000 – New connections per second: 135000
11	شرط رفض	Features	– Modular design – firewall protection – VPN support – Intrusion Prevention System (IPS) – web threat protection – two bypass interface pairs
17		guarantee	Not less than a full Gregorian year

5.2.6. المواصفة الفنية لوحدة التخزين الشبكية (NAS Storage)

#	شرط رفض	اسم المواصفة	المواصفة الفنية المطلوبة
1		الماركة والطراز	- من إنتاج إحدى الشركات العالمية المتخصصة في هذا المجال والمعروفة بجودة منتجاتها العالية في السوق العالمية. - يطلب من العارض تحديد الماركة والطراز.
2		Type	Rack Mount
3	شرط رفض	CPU	8 core
4	شرط رفض	RAM	8 GB Expandable
5	شرط رفض	Disk Bays	16 minimum
6	شرط رفض	Usable Capacity	100 TB Minimum
7		External Ports	2 x RJ-45 1GbE LAN Port 2 x RJ-45 10GbE LAN Port

5.2.7. المواصفات الفنية المطلوبة لقطع التبديل والتوسعة

(يوجد حاجة لمجموعة من قطع التبديل والتوسعة المتوافقة مع المخدمات الموجودة حالياً في الوزارة، وهي من ماركة HP)

#	اسم المواصفة	المواصفة الفنية المطلوبة	العدد المطلوب
1	RAM	HP 16GB (1x16GB) Dual Rank x4 PC3-14900R(DDR3-1866) Registered CAS-13 Memory Kit	16
2	RAM	HPE 16GB (1x16GB) Single Rank x4 DDR4-2400CAS-17-17-17 Registered Memory Kit	8
3	Network interface	HP Ethernet 1Gb 4-port 331T Adapter	3
4	HDD	HP 1.2TB 12G SAS 10K rpm SFF (2.5-inch) SC Enterprise 3yr Warranty Hard Drive	6

#	اسم المواصفة	المواصفة الفنية المطلوبة	العدد المطلوب
5	HDD	HPE 1.2TB SAS 12G Enterprise 10K SFF (2.5in) SC 3yr Wty Digitally Signed Firmware HDD	3
6	SSD	HP 960GB 6G SATA Mixed Use-3 SFF 2.5-in SC 3yr Wty Solid State Drive	2
7	SSD	HPE 960GB SATA 6G Mixed Use SFF (2.5in) SC 3yr Wty Digitally Signed Firmware SSD	1

5.3. متطلبات التركيب والتشغيل

1. على الشركة المنفذة التقيد بالمكان المخصص لتركيب وتشغيل المنظومة في مركز المعطيات الوطني في الهيئة.
2. على الشركة المنفذة توريد وتركيب برمجيات الأنظمة التي تحتاج إليها المنظومة.
3. على الشركة المنفذة تسليم كل ما يتعلق بالمنظومة من أدلة الاستخدام، وأدلة إدارة النظام، وأدلة الدعم الفني الأولي.
4. يتم تحديد متطلبات التشغيل بناء على اتفاقية مستوى الخدمة يجري الاتفاق عليها وتوقيعها مع الهيئة عند بدء المرحلة الرابعة.

5.4. متطلبات التدريب

1. على العارض تقديم مقترحه لبرنامج التدريب على أن يتضمن التدريب على إدارة المكونات البرمجية للمنظومة.
2. ملاحظة: سيتم تحديد أعداد المتدربين لاحقاً، ويجب أن تراعي برامج التدريب المقترحة النقاط التالية:
   - الاعتماد على المناهج المعتمدة ومراكز التدريب المعتمدة ما أمكن.
   - تحديد المؤهلات للمتدربين بشكل واضح.
   - برامج التدريب الزمنية تحدد بشكلها النهائي بالاتفاق مع الهيئة.
   - يشمل التدريب حالات عملية حقيقية ينفذها المتدربون تحت إشراف المدربين.

5.5. متطلبات الصيانة والدعم الفني

1. تلتزم الشركة المنفذة بضمان صيانة التجهيزات والمكونات البرمجية مجاناً لمدة سنة اعتباراً من تاريخ الاستلام المؤقت.
2. يجب أن تتضمن عمليات الصيانة كل من:
   - إزالة الأخطاء من المكونات البرمجية أو إعداداتها أينما ظهرت.

- إصلاح أو صيانة الأعطال في التجهيزات العتادية أينما ظهرت.

3. يجب إزالة الأخطاء في المكونات البرمجية أو إعداداتها التي تعيق الأعمال في مدة لا تتجاوز 4 ساعات، ويمكن أن تصل المدة إلى 12 ساعة من تاريخ الإبلاغ عن الخطأ في حال كان العطل لا يعيق العمل.
4. يجب أن تقدم الشركة المنفذة فريق دعم فني لمدة سنة ميلادية كاملة بعد الاستلام المؤقت للمنظومة.
5. يجب أن تقدم الشركة المنفذة الدعم الفني للمنظومة على الهاتف خلال أوقات الدوام الرسمي لمدة سنة ميلادية كاملة بعد الاستلام المؤقت للمنظومة.

6. التزامات العارض (متطلبات العرض)

تعبر الفقرة التّالية عن إطار العمل المطلوب من العارض، وعليه الالتزام به لتحقيق المتطلبات المحددة في دفتر الشروط، وفي حال كان لدى العارض أية استفسارات أو ملاحظات تتعلق بإطار العمل، أو بالمتطلبات، فعليه توجيه استفساراته خطياً قبل ما لا يقل عن خمسة عشر يوماً من الموعد المحدد لتقديم العروض، ويعود للوزارة إرسال الإجابات عن الاستفسارات خطياً لجميع العارضين المحتملين (الحاصلين على دفتر الشروط)، أو الدعوة لاجتماع أو أكثر وتثبيت النقاط العالقة في محضر اجتماع، علماً بأن اختبار القبول سيجري وفقاً للمتطلبات المحددة في فقرة توصيف متطلبات المشروع، بالإضافة لأية توضيحات على المتطلبات أو على إطار العمل المحدد للعارض يجري إرسالها أصولاً من قبل الوزارة.

6.1. آلية تقييم العروض

تجري عملية تقييم العروض بناء على النقاط الآتية:

1. الوفاء بجميع المتطلبات الواردة في هذه الوثيقة، وأينما كان ورودها.
2. الجودة الفنية للحل المقدم (المواصفات الفنية للتجهيزات العتادية والمكونات البرمجية والنظم المستخدمة في تصميم الحل المقترح).
3. البنية التقنية للحل المقترح Architecture، وقدرته على تحقيق المتطلبات التقنية.
4. نتائج العرض التقديمي و Live Demo الذي يجريه العارض عن تصور الحل المقترح، ومجموعة الأعمال السابقة المشابهة لهذا المشروع من حيث حجم العمل ودرجة التعقيد وحساسية دوره، وألا يكون لديه مشاريع فاشلة أو معلقة بسببه.
5. خبرات فريق العمل وهيكليته، وكذلك وجود خبرات كافية والمهندسين ومديري المشاريع للوفاء بمتطلبات المشروع (يجب أن يكون مدير المشروع في الشركة العارضة مُجاز (certified) من الشركة الأم التي تقدم هذا الحل).
6. منهجية التنفيذ وخطته والجدول الزمني لخطوات التنفيذ.
7. الاعتبارات الأمنية للمنظومة.
8. كيفية معالجة العارض لإدارة المخاطر ضمن المشروع.

9. مقترحات العارض لتوسيع استخدام المنظومة من قبل المستفيدين.

<u>وتعتبر النقاط التالية نقاط تستدعي رفض العرض المقدم دون تقييمه:</u>

1. العرض غير المتضمن التزام العارض بتقديم كامل المكونات الأساسية للمنظومة.
2. العرض المقدم من شركة لا تعمل في مجال تكنولوجيا المعلومات.

6.2. خبرة وكفاءة العارض

يجب على الشركة العارضة أن تقدم سيرة ذاتية مفصلة تبين فيها خبرتها في مجال تطبيقات الشبكية وأنظمة مراكز البيانات المعرفة برمجياً (SDDC).

يجب أن تتضمن السيرة الذاتية المفصلة البنود التالية:

1. نبذة عن تاريخ الشركة العارضة، والمشاريع/الأنظمة التي قامت بتنفيذها مع شرح موجز عن أهم التطبيقات التي قامت الشركة بتطويرها أو التي تعمل على تطويرها.
2. لائحة بجهات القطاع العام والخاص والمشترك والمنظمات الدولية التي تعاقدت مع الشركة العارضة على توطين الأنظمة الآنفة الذكر فيها، إضافة إلى عناوين هذه الجهات وأرقام الهواتف.
3. لائحة بأسماء العاملين في الشركة وسيرهم الذاتية.
4. لائحة بأسماء فريق العمل المتفرغ للمشروع وسيرهم الذاتية التي توضح لمحة موجزة عن خبراتهم العلمية والعملية. كما يجب تحديد <u>اسم مدير المشروع</u> الذي سيتم التعامل معه خلال مراحل العمل، مع تعهد بتفرغهم الكامل للمشروع أثناء التنفيذ.
5. الإجراءات المتبعة في إدارة المشاريع لدى الشركة.

<u>وفيما يلي الحد الأدنى من متطلبات الخبرة:</u>

1. يجب أن تمتلك الشركة مجموعة من العناصر الفنية المتخصصة في هذا المجال، على ألا يقل عدد ذوي الخبرة منهم التي تزيد عن خمس سنوات عن 3 عناصر.
2. يفضل أن يكون مدير المشروع في الشركة العارضة مُجاز (certified) من الشركة الأم التي تقدم هذا الحل (ترفق صورة عن الشهادة المطلوبة في حال وجودها).
3. يجب على العارض أن يبين خبرة شركته في تطوير منظومات مماثلة، وأن يقدم قائمة بالمشاريع الناجحة التي نفذها أو ينفذها.

6.3. الحل المقترح

6.3.1. تغطية الحل المقترح للمتطلبات

1. يجب على العارض الالتزام بجميع المتطلبات المذكورة في هذا الدفتر، كما يجب على العارض شرح وتوضيح كيفية الالتزام بالمتطلبات في الحالات التي يُطلب فيها ذلك.
2. يجب على العارض تقديم عرض تقديمي و Live Demo يوضح تصوره للحل المقترح، أثناء مرحلة تقييم العروض.
3. يمكن للجنة الدارسة للعروض طلب توضيحات على العروض وطرح أي سؤال فني، وعلى العارض توثيق هذه التوضيحات حيث تعتبر جزءاً لا يتجزأ من العرض.
4. على العارض أن يجيب على كل بند من بنود دفتر الشروط الفنية ضمن عرضه الفني وبالتفصيل، مع ذكر المعايير والأدوات التي يستعملها.

6.3.2. تصميم الحل

1. يجب أن يصف العارض البنيان التصميمي للحل المقترح وكيفية تغطية هذا البنيان لجميع المتطلبات، ويجب توضيح البنيان بمخططات بيانية. كما يجب تحديد البنية التحتية المستخدمة للتطوير وللتشغيل.
2. على العارض أن يقدم معلومات عن كافة البرامج والأدوات التي سيستخدمها في تنفيذ المكونات البرمجية.

6.3.3. إدارة وتنظيم المشروع

1. يجب أن يقدم العارض خطة إدارة المشروع.
2. يتم تحديد بنية فريق عمل الشركة المنخرط في المشروع والأدوار وتوزيع المسؤوليات على هذه الأدوار. ويجب على العارض تقديم المخطط التنظيمي للمشروع مبيناً متطلبات التنظيم من جانب الجهة المستفيدة ومن جانب العارض.

6.3.4. الالتزامات القانونية

لا يسمح للعارض بإضافة أية برمجيات أو بيانات خاصة ذات غرض تجاري، أو تهدف إلى الترويج له أو لشركة أخرى على المنظومة، وبالتالي يمنع استخدام المنظومة لتقديم أية خدمات لا تتم الموافقة عليها من قبل إدارة المنظومة. كما لا يجوز الإشارة إلى أي علامة تجارية ترتبط بالعارض مباشرة أو بشكل غير مباشر، ولا يجوز إدراج أي رابط ذي صفة تجارية دون الحصول على موافقة إدارة المنظومة.

6.3.5. المراحل والجدول الزمني

1. يجب على العارض وضع خطة زمنية متقيدة بالإطار الزمني المحدد للمشروع.

2. في حال إنجاز إحدى المراحل ضمن فترة أقل من الفترة المحددة لها يحق للشركة المنفذة الاستفادة من المدة المحددة للمرحلة وإضافتها إلى المدة الخاصة بالمرحلة التالية ضمن خطة العمل، شرط استيفاء شروط استلام المرحلة المعنية ومصادقة لجنة الإشراف على المشروع على ذلك.

7. هيكلية الوثائق المطلوبة

7.1. بنية العرض الفني

على العارض تقديم عرضه بحيث يكون العرض مقسماً ومرقماً وفق التالي:

1. صفحة الغلاف.
2. جدول المحتويات.
3. الملخص.
4. لمحة عن الشركة العارضة وخبراتها.
   - 4.1 اسم وعنوان الشركة مقدمة العرض.
   - 4.2 وصف الشركة (ترفق وثيقة تأسيس الشركة).
   - 4.3 مخطط الهيكل التنظيمي للشركة.
   - 4.4 اسم مدير الشركة (رقم الهاتف والبريد الإلكتروني).
   - 4.5 اسم شخص الاتصال المسؤول عن العرض (رقم الهاتف والبريد الإلكتروني).
   - 4.6 عدد سنوات خبرة الشركة في تطوير وصيانة وتشغيل منظومات مشابهة (من حيث حجم الخدمات والمستخدمين).
   - 4.7 قائمة بالأعمال المماثلة السابقة.
   - 4.8 السير الذاتية للمشاركين في المشروع (المنصب في المشروع، المؤهلات العلمية، الخبرات العلمية ذات الصلة، الشهادات، وصف المشاريع التي شارك بها).
5. الحل المقترح من قبل العارض.
   - 5.1 نظرة عامة.
   - 5.2 وصف مفصل للحل المقترح.
     - 5.2.1 البنية الفيزيائية المطلوبة لتنفيذ المنظومة.
     - 5.2.2 توزيع الأنظمة الجزئية وترابطها.
   - 5.3 ملاحظات على نطاق العمل، والتغييرات المقترحة على المتطلبات (إن وجدت).
   - 5.4 الالتزام بالمتطلبات الوظيفية والتقنية (يجب إرفاق جدول بالمتطلبات يوضح بيان كيفية تحقيق كل منها).
6. منهج تنفيذ النظام.

6.1 خطة تطوير المنظومة.

6.2 خطة الاستلام المؤقت.

6.3 إدارة المشروع في مراحله المختلفة.

6.4 الجدول الزمني لتنفيذ المشروع.

6.5 خطة الصيانة والدعم الفني.

6.6 خطة التشغيل.

6.7 خطة التدريب.

8. الملاحق

- ملحق رقم 1: جدول تحليل الأسعار الإفرادية والإجمالية الخاصة بالأعمال المطلوبة.

9. توقيع اللجنة

عضواً	عضواً	عضواً	رئيساً
خالد فرج	م. بريفان حمعة	م. حيان صالح	م. بيان الحللي

شوهد

معاون وزير الاتصالات والتقانة

المهندسة فاديا سليمان

صدق

وزير الاتصالات والتقانة

المهندس إياد الخطيب

ملحق 1: جدول تحليل الأسعار الإفرادية والإجمالية

لمشروع توريد وتركيب وتشغيل منظومة الحوسبة السحابية

#	البند	السعر الإفرادي	العدد	السعر الإجمالي
1	المرحلة 1: توريد وتركيب التجهيزات المطلوبة			
1.1	المخدم		5	
1.2	مبدل Switch 10G		4	
1.3	مبدل Switch 1G		4	
1.4	جدار ناري Next Generation Firewall		2	
1.5	وحدة التخزين الشبكية NAS Storage		1	
1.6	الذواكر RAM HP 16GB Dual Rank		16	
1.7	الذواكر RAM HP 16GB Single Rank		8	
1.8	كرت شبكة		3	
1.9	قرص صلب HDD 1.2 TB		6	
1.10	قرص صلب SSD 960GB 6G SATA Mixed		2	
1.11	قرص صلب SSD Digitally Signed Firmware		1	
2	المرحلة 2: تنفيذ مركز البيانات المعرف بشكل برمجي		1	
3	المرحلة 3: تنفيذ مكون إدارة البنية السحابية ونظام إدارة المعلومات وأحداث الحماية والأمن		1	
4	المرحلة 4: التشغيل والتدريب		1	
	الكلفة الإجمالية			

توقيع وخاتم الشركة